

**WORKPLACE DISCIPLINE
AND
THE RIGHT TO PRIVACY**

**Submitted as the dissertation component (which
accounts for 50% of the degree) in partial fulfilment
of the requirements for the degree of LLM in the
Faculty of Law, University of Kwa Zulu Natal.**

By Masego Magdaline Mookodi

The Bindery, Gaborone

February 2004

Acknowledgements

This dissertation was made possible through the support of many and I would like to acknowledge and thank the following individuals for their support.

My supervisor and former lecturer Prof Alan Rycroft who was always understanding of the challenges I was faced with in trying to balance my new job and doing my dissertation at the same time.

My boss Mrs Dorcas Makgato Malesu for approving my leave on numerous occasions despite the fact that I had been working for her for less than a year and still trying to find my ground.

The Commissioner of Labour and a personal friend indeed Mr Claude Mojafi, for his invaluable input despite the short period of time he had within which to read the dissertation.

Dr Maude Dikobe for taking time off her busy schedule to edit my work.

Last but not least I would like to express my sincere gratitude to my mother and friend Emily Motlalepula Mookodi whose patience and love never ceases to amaze me.

Lastly I would like to thank the Almighty Lord for giving me the strength to complete this work.

ACKNOWLEDGEMENTS.....	i
TABLE OF CONTENTS.....	ii
TABLE OF CASES.....	iii
1. INTRODUCTION.....	1
2. THE RIGHT TO PRIVACY.....	3
2.1 The meaning of privacy.....	4
2.2 Constitutional right to privacy.....	5
2.3 Legitimate expectation of privacy.....	6
2.4 The right to be left alone.....	9
2.5 The right to the development of the individual personality.....	10
2.6 Informational privacy.....	10
2.7 Limitation of the right to privacy.....	11
2.8 Searches and seizures.....	13
2.8.1 The constitutionality of laws authorising searches and seizures.....	13
2.9 Infringement of Privacy: Wrongfulness.....	14
2.10 Intrusion or acquaintance.....	15
2.11 Disclosure or Revelation.....	15
2.12 Justifying a right of employee privacy.....	20
2.20 Conclusion.....	23
3. MANAGEMENT PREROGATIVE.....	24
3.1 The term management prerogative.....	25
3.2 The legal basis of management prerogative.....	26
3.3 The purpose of management prerogative in an establishment.....	30

3.4	The scope of employer prerogative.....	30
3.4.1	An industrial relations perspective on the scope of employer prerogative.....	31
3.4.2	Employers' perspective on the scope of their prerogative...32	
3.4.3	A labour law perspective on the scope of the employer prerogative.....	33
3.5	Workplace Forums.....	34
3.6	Conclusion.....	34
4.	WORKPLACE DISCIPLINE.....	37
4.1	The guidelines in respect of the employees right to discipline.....	38
5.	WORKPLACE DISCIPLINE AND TELEPHONE ABUSE.....	39
5.1	The Interception and Monitoring Prohibition Act 127 of 1992.....	40
5.2	Admissibility of telephone recordings.....	42
5.3	Common Law and Admissibility of illegally obtained evidence...46	
5.4	Constitutional Right to Privacy and Monitoring	47
5.5	Waiving of Rights.....	49
5.6	Issue of Company Property.....	50
5.7	Issue of Company Time.....	52
5.8	Issue of Loyalty and Honesty.....	53
5.9	Conclusion.....	53
6.	WORKPLACE DISCIPLINE AND INTERNET ABUSE.....	55
6.1	An Internet User Policy.....	55
6.2	Employee Privacy and Internet Usage.....	57
6.3	Reasons for monitoring the Internet.....	60
6.3.1	Company Time.....	60

6.3.2	Clogging the corporate network.....	61
6.3.3	Expressly prohibited use.....	62
6.3.4	Gender and Racial issues.....	62
6.3.5	Vicarious Liability.....	63
6.3.6	Performance Monitoring.....	65
6.3.7	Property of the employer.....	65
6.3.8	Personal Use.....	66
6.4	Conclusion.....	66
7.	WORKPLACE DISCIPLINE AND ELECTRONIC SURVEILLANCE...	68
7.1	The implied duty of mutual trust and confidence.....	69
7.2	The role of videotapes as evidence of misconduct.....	71
7.3	Defence of Property.....	72
7.4	Conclusion.....	72
8.	ADMISSIBILITY OF AND POLYGRAPH TESTING AT THE WORKPLACE.....	75
8.1	Conclusion.....	76
9.	CONCLUSION.....	77

TABLE OF CASES

1. Allied Workers Union of SA on behalf of Neube v Northern Crime Security CC
(1999) 20 ILJ 1954 (CCMA)
2. Antonette Dorfling Union v Precision Sharpening Services CC unpublished
CCMA Case no KN 15866
3. Bamford & Others/ Energizer (SA) Ltd (2001) 12 BALR 1251
4. Bernstein v Bester 1996 (2) SA 751 (CC) para 67
5. Case v Minister of Safety and Security 1996 (3) SA 165 para 19
6. Checkers SA Ltd (South Hills Warehouse) & SA Commercial Catering & Allied
7. Cronje v Toyota Manufacturing (2001) 22 ILJ 735 (CCMA)
8. D S Sosibo & others and CTM (2001) 22 ILJ 811(CCMA) P817
9. Frances Hasessan Jones v Eccles Associates Case No not stated
10. George v Liberty Life Association of Africa (1996) 17 ILJ 571 IC, 582
11. Goosen v Caroline Frozen Yoghurt Parlour (1995) 16 ILJ 296 (IC)
12. Haford v United Kingdom (1997) IRLR 47 (ECHR)
13. High Court in Park-Ross v Director Office for Serious Economic Offences 1995
(2) BCLR 198 (C)
14. Hunter v Southam Inc 11 DLR (4th) 641
15. Investigating Directorate; Serious Economic Offences v Hyundai Motor
Distributors 2000 (10) BCLR 1079 (CC)
16. Jacob v Unitrans Engineering (1999) KN219..1,
17. Long Beach City Employees Association v Long Beach 719 P 2d 660 (cal. SC
1986) 672
18. Mistry v Interim Medical and Dental Council of South Africa (1998) SA 1127
(CC) 27

19. Mhlangu v CIM Delta ILJ Vol 21 Jan 2000
20. Mhlongo v Bailey 1958 1 SA 370 (W)
21. Mkhize and Bayhead Cold Storage Unreported CCMA award
22. Mncube v Cash Paymaster Services (Pty) Ltd (1997) 5 BLLR 639 (CCMA)
23. Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA)
24. Katz v US 389 US 347 (1967)
25. Motor Industry Fund Administrators (Pty) Ltd v Janit 1994 (3) SA 56 (W)
26. National Media Ltd v Bogoshi 1998(4) SA 1196 (SCA)
27. O'Connor v Ortega 107 S Ct. 1492 (1989) 76
28. O'Connor v Ortega 480 US 709 (1987)
29. Olmstead v The United States 277 US 438 (1927)
30. Protea Technology Ltd and Another v Wainer and Others 1997 (9) BCLR 1225
(W) AT 1237 D-E
31. SACCAWU obo Sydney Fongo v Pick 'n' Pay Supermarket (2000) FS 15555
32. Katz v United States 389 US 347 (1967)
33. S v Bhulwana 1996(1) SA 388 (CC)
34. Tap Wine Trading v Cape Classic Wines 1999 (4) SA 194
35. UFCW, Local 1400 v Saskatchewan Co-Operative Association Ltd (1992) 101
Sask. R I (QB)
36. Warren Thomas Griffiths Union v VWSA unpublished CCMA case no KN EC
16174
37. Workers Union 1990 11 ILJ 1357 (ARB) 1365 I

1 INTRODUCTION

This thesis seeks to critically interrogate whether electronic surveillance, internet monitoring, telephone tapping and polygraph testing can be regarded as a violation of the right to privacy. It further interrogates workplace disputes arising from these practices. The thesis will rely on various cases to illustrate the different situations where it was found justifiable to 'invade' privacy as well as situations where it was found unjustifiable. This invasion to privacy will also be linked to management prerogative to manage in relation to the right to privacy.

The right to privacy is a concept that has not been in existence for a long time, especially in the employment context. However it has recently attracted much attention as people become more and more technologically oriented. Unfortunately technology by its nature makes it easy for those aspects of employment that are traditionally regarded as part of the domain of an employee privacy to be accessible to others.

In addition the employment relationship by its nature dictates that there are those who manage and those who are managed. Those who manage have certain prerogatives that are inherent in the nature of their responsibility. However human beings have certain expectations values and rights. The right to privacy may be regarded as one of the most comprehensive and valued right by persons in the 21st Century. It is crucial not to disregard the fact that the right to privacy, like all the other, rights is not absolute. When an employee enters the domain of the workplace he or she should not expect the same degree of privacy that may be enjoyed in the domain of their home. The law provides that the employer has the right to manage the work carried out by

employees at the workplace but pays little account to the right to privacy of employees.

The thesis will consider the following topics

- 1) The right to privacy in general
- 2) Managerial Prerogative at the workplace
- 3) Workplace Discipline by management
- 4) Workplace Discipline and Telephone Abuse
- 5) Workplace Discipline and Internet Abuse
- 6) Workplace and Electronic Surveillance
- 7) Workplace discipline and polygraphic testing
- 8) Conclusion

In conclusion, there will be a discussion of the various aspects that are of paramount importance in determining whether there has been invasion of privacy in the execution management responsibility as well as the possible challenges facing both employers and employees..

2 THE RIGHT TO PRIVACY

The right to privacy is a relatively new legal concept. Legal decisions supporting privacy were based on property rights and contracts. An independent right to privacy was not recognised. According to Baase,¹ an article called 'The Right to Privacy' was written in 1890 by Samuel Warren and Louis Brandeis (later a Supreme Court Justice) which argued that privacy was distinct from other rights and needed more protection. In the decision of *Olmstead v The United States*² Justice Brandeis held that 'privacy is the right to be left alone; the most comprehensive right and the most valued by civilised men' - a legal shield which could be asserted by the individual against the prying eyes of the public. In the employment context it is viewed as the appropriate concept for guiding the regulation of aspects of employment relationship, particularly the use by management of certain techniques, such as monitoring of electronic communication.

Faleri³ mentions that in the legislation of all European Union member states the right to privacy is not seen simply as a right which must not be infringed by third parties, but rather as a right of data subjects to decide and to supervise the use that is made of their own personal data: the legislature clearly wishes to give the data subject an active role.

The fact that privacy has emerged as an important societal virtue is demonstrated by the inclusion of the right against arbitrary interference with privacy Article 17 of the

¹ S Baase *A Gift of Fire* (1997) 64

² *Olmstead v The United States* 277 US 438 (1927)

³ Faleri C *Comparative Labour Law and Policy Journal*; Information Technology and Workers Privacy Public and Private Regulation' Vol 23, No2, Winter 2002, 520

International Covenant on Civil and Political Rights. The Right to Privacy appears in Article 11 of the American Convention on Human Rights. It is a fundamental right protected by the Legal Order of the European Union.

2.1 The meaning of privacy

Privacy is a basic human need that is fundamental to the development and advancement of both a free society and a mature and stable personality for an individual⁴. This right is valued as a right by persons, both in relation to intrusion by the state and as far as other people is concerned. It is also a right which is inextricably intertwined with human dignity. The right to privacy is therefore based on human dignity and has as its objective the preservation for each individual of the choice of when and how much he or she will allow others to know about his or her activities.

Remp⁵ mentions that the Office of Technology Assessment (OTA) in its 1994 Congressional Report stated that

Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information.

Neethling⁶ on the other hand states that;

Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all the personal facts which the person

⁴ G.E Devenish *A Contemporary on the South African Bill of Rights* (1999) 135

⁵ M Remp Ann *The 21st Century: Meeting the Challenges to Business Education* (1999) 117

himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy.

Cockhead⁷ maintains that it would appear like this definitions of the modern law of invasion of privacy, arose out of a need to protect the individual's dignity and mental tranquility of people in a sophisticated and developing society where technology has enabled the former boundaries of privacy to be invaded.

2.2 Constitutional right to privacy

The right to privacy in South Africa is set out in Section 14 of the Constitution⁸ as follows;

Everyone has the right to privacy which includes the right not to have-

(a) their possession or home searched

(b) their property searched

(c) their possessions seized or

(d) the privacy of their communication infringed

Section 14 is divided into two parts. The first part guarantees a general right to privacy and the second protects against specific infringement of privacy, namely searches and seizures and infringements of the privacy of communication. In most cases searching of one's person, home, or property or intercepting one's communication will result in infringement of Section 14. Nevertheless since the protection against searches and seizures is a subordinate element of the right to privacy, the constitution's protection is triggered only when an applicant shows that a

⁶ Neethling et al *Neethling's Law of Personality* (1996) 36

⁷ A Cockhead *A Critical Analysis of Law of Privacy With Reference To Invasion Of Privacy Of Public Figures* (1990) 5

⁸ Constitution of the Republic of South Africa Act 108 of 1996 (1996 Constitution)

search, seizure or interception of communication has infringed the general right to privacy⁹.

2.3 Legitimate expectation of privacy

A legitimate expectation of privacy entails that one must have a subjective expectation of privacy that society recognizes as objectively reasonable¹⁰. The subjective expectation component recognizes that nobody can complain about an infringement of privacy if they have consented explicitly or implicitly in having their privacy invaded. Consequently it is difficult to assess the kinds of privacy expectation that society would regard as objectively reasonable.

The Constitutional Court provided some guidelines with regard to the issue of reasonable objectivity. In *Bernstein v Bester No¹¹* which dealt with personal privacy and the right not to be subject to the seizure of private possessions or the violation of private communication, the court observed;

The truism that no right is to be considered absolute implies that from the outset of interpretation, each right is always limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preferences and home environment which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged

⁹J De Waal, Currie I & Erasmus G; *The Bill of Rights Handbook* (2001) 268

¹⁰ Collier D 'Workplace Privacy in the Cyber Age' *ILJ* 2002 Vol 23 October 1750

in the truly personal realm but as a person moves into communal relations and activities such as business and social interaction, the scope of the personal space shrinks accordingly.

With due respect the Court in *Bernstein* was more or less stating the obvious. What needed a closure and comprehensive interrogation was the extent to which limitation of substantive right is permissible. Emphasis should also have been given to the cultural context of the right to privacy. This is crucial because in communitarian societies such as those found in Africa, the right to privacy is seriously compromised because the concept of individuality is alien to societal values.

To illustrate this point in the judgement of *Mistry v Interim Medical and Dental Council of South Africa*¹² the court emphasised, in relation to business undertakings, that the more public the undertaking and the more closely regulated, the more attenuated would the right to privacy be and the less intense any possible invasion. It also stated that in the case of any regulated business enterprise, the proprietor's expectation of privacy in relation to the premises, equipment, materials and records must be attenuated by the obligation to comply with reasonable regulations and to tolerate the administrative inspections that are an integral part of an effective regime of regulation. People involved in such an undertakings must know from the beginning that their activities will be monitored. The Court referred to a Canadian judgement where this point was well articulated:

¹¹ *Bernstein v Bester* 1996 (2) SA 751 (CC) para 67

¹² *Mistry v Interim Medical and Dental Council of South Africa* (1998) SA 1127 (CC) 27

The degree of privacy the citizen can reasonably expect may vary significantly depending on the activity that brings him or her into contact with the state. In a modern industrial society it is generally accepted that many activities in which individuals can engage must nevertheless to a greater or lesser extent be regulated by the state to ensure that the individual pursuit of his or her self-interest is compatible with the community's interest in the realisation of collective goals and aspirations.

In *Investigating Directorate; Serious Economic Offences v Hyundai Motor Distributors*¹³ the Court held that, the statements in *Berstein* and presumably in *Mistry* do not mean that the people no longer retain a right to privacy in the social capacities in which they act. Therefore, when people are in their offices, in their cars or on mobile telephones they still enjoy the right to be left alone by the state unless certain conditions are met.

De Waal¹⁴ states that, the right to privacy seeks to protect three related concerns:

(2.3.1) the right to privacy seeks to protect certain aspects of one's life in respect of which one is entitled to be left alone; one's body, certain places such as one's home and certain relationships such as marital sexual or other intimate relationships.

(2.3.2) It also aims to protect the opportunities for an individual to develop his or her personality and therefore extends to certain forms of individual and personself realisation or self fulfillment.

(2.3,3) It seeks to protect the ability of individuals to control use of private information about themselves.

¹³ *Investigating Directorate; Serious Economic Offences v Hyundai Motor Distributors* 2000 (10) BC1.R 1079 (CC)

¹⁴ De Waal (refer note 9 above) 270

The right to privacy also enables one to develop and maintain relations with other human beings so as to satisfy one's ability to relate to oneself.

2.4 The Right to be left alone

The right to be left alone is deemed as an important part of privacy when it comes to an individual's body, home and family life¹⁵. The rationale behind this right is that the state and other people should have nothing to do with other people's intimate affairs¹⁶.

The right to privacy recognizes that every individual is entitled to a sphere of personal autonomy in which the law may not interfere. In the judgement of *Case v Minister of Safety and Security*¹⁷ the Court stated that:

what erotic material I may choose to keep within the privacy of my home, and only for my personal use there, is nobody's business but mine. It is certainly not the business of society or the state. Any ban imposed on my possession of such material for that solitary purpose invades the personal privacy which s13 of the Interim Constitution guarantees that I shall enjoy.

It must be emphasised however that there may be situations when society has a legitimate expectation to know what an individual possesses because sometimes the interest of the individual and society are intertwined. In emerging constitutional democracies characterised by conservative attitudes the right to privacy needs to be conceptualised and be broadly construed and applied. It would not be consistent with the contemporary move of societies in emerging constitutional democracies to give

¹⁵ See Universal Declaration of Human Rights (1948) article 12 which states that no one shall be subjected to arbitrary interference with his privacy, family or home or correspondence, nor to attacks upon his honour and reputation. Everybody has the right to the protection of the law against such interference or attacks

¹⁶ De Waal (refer note 9 above) 271

¹⁷ *Case v Minister of Safety and Security* 1996 (3) SA 165 para 19

the right to privacy blanket permission. The emerging constitutional democracies seek to protect those areas that are considered to be of great societal concern such as child pornography.

2.5 The Right to the development of the individual personality

Protection of privacy is fundamental for the individual to develop his/her personality. The right to privacy protects the right of individuals to be or become, at the personal level, the kind of person they want to be. The right to the development of the individual personality includes among other things; the type of clothes one chooses to wear, inscribed tattoos on their bodies and hairstyles. The concept of privacy includes the right to institute and maintain relations with other human beings for the satisfaction of one's personality or the ability of a person to relate to oneself and to integrate with others in a worthwhile manner¹⁸.

2.6 Informational privacy

Protection of privacy is also crucial to protecting human dignity in the sense that it guarantees the right of a person to have control over the use of private information. Hence informational privacy is closely related to the right to dignity due to the fact that publication of embarrassing information or information which places a person in a false light has negative implications to the dignity of that person¹⁹.

In its judgement in the *Mistry*²⁰ case the Constitutional Court cited some factors which it considered imperative when dealing with informational privacy. The factors are as follows; whether the information was obtained in an intrusive manner; whether

¹⁸ De Waal (refer note 9 above) 275

¹⁹ Ibid 276

it was about intimate aspects of the applicant's personal life; whether it involved data provided by the applicant for one purpose which was then used for another; whether it was disseminated to the press or the general public or persons from whom the applicant could reasonably expect such private information would be withheld.

2.7 Limitation of the right to privacy

The right to privacy is not absolute, and like all Chapter Two rights in the Constitution it is subject to reasonable and justifiable limitations or restrictions in terms of section 36 of the Constitution, by a law of general application to the extent that it is reasonable and justifiable in an open and democratic society, based on human dignity, equality and freedom, taking into account all relevant factors including those mentioned in the section.

When dealing with the issue of legitimacy of limitation the Constitutional Court's view was articulated in *Sv Makwanyane*²¹ decision. In that judgement the Court held as follows;

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. This is implicit in the provisions of s33 (1) (IC). The fact that different rights have different implications for democracy, and in the case of our constitution for an open and democratic society based on 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

²⁰ *Mistry v Interim Medical and Dental Council of South Africa* (note 12 above) para 51

²¹ *Sv Makwanyane* 1995 (3) SA 391 (CC) para 104

done on a case by case basis. This is inherent in the requirement of proportionality, which calls for the balancing of different interests. In the balancing process, the relevant considerations will include the nature of the right that is limited and the importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy and particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question. In the process regard must be had to the provisions of s33(1)(IC), and the underlying values of the Constitution, bearing in mind that, as a Canadian Judge has said, ‘the role of the Court is not to second-guess the wisdom of policy choices made by the legislators.

This paragraph has been summarized in *S v Bhulwana*²² as follows;

In sum, therefore, the court places the purpose, effects and importance of the infringing legislation on one side of the scales and the nature and effect of the infringement caused by the legislation on the other. The more substantial the inroad into fundamental rights, the more persuasive the grounds of justification must be.

The above quotations indicate that rights can only be limited if the party that is infringing the right demonstrates that infringement is for very compelling reasons²³. A compelling good reason is that the infringement serves a purpose that is considered legitimate by all reasonable citizens in a constitutional democracy. The infringement

²² *S v Bhulwana* 1996(1) SA 388 (CC) para 18

²³ See European Convention on Human Rights Article 18

must however not impose costs that are disproportionate to the benefits that it obtains²⁴.

2.8 Searches and seizures

Searches and seizures involve a violation of a person's right to privacy. They must only be concluded in terms of legislation that defines the power to search and seize. The person conducting the search has to be issued with a search warrant. Any search that does not have authority would be a constitutional violation. The other requirement of reasonable grounds for justification was addressed in the *Hyundai*²⁵ judgement whereby the Constitutional Court held that for purposes of a preparatory investigation, a search and seizure would not be constitutionally justifiable in the absence of a reasonable suspicion that an offence had been committed.

2.8.1. The constitutionality of laws authorising searches and seizures

The Criminal Procedure Act²⁶ is the most important law which authorises searches and seizures. Whereas the Act contains provisions, which are deemed in some quarters to violate the right to privacy, such provisions are subject to the limitation clause. There has to be compliance with Section 36 of the Constitution according to which the authorizing law must properly define the scope of the power to search and seize. There also has to be prior authorisation of the search and seizure by an independent authority. The Act also requires an independent authority to be persuaded by evidence on oath that there are reasonable grounds for conducting the search.

²⁴ De Waal (refer note 9 above) 162

²⁵ *Investigating Directorate; Serious Economic Offences v Hyundai Motor Distributors* (refer note 13 above)

²⁶ Criminal Procedure Act of 1977; Section 21 (2)

The issue of prior authorization was addressed by the *High Court in Park-Ross v Director Office for Serious Economic Offences*²⁷ where the offices of a company were raided and documents seized and copied in terms of section 6 of Serious Economic Offences Act 117 of 1991. The seizure was effected after the Office of Serious Economic Offences decided to hold an enquiry in terms of section 5 of the Act. The Court held that section 6 of the Act constituted a violation of the right to privacy as embodied in Section 131C. The Court findings were based on the fact that the value protected by the law of search and seizure as in the United States and Canada is privacy rather than property²⁸.

2.9 Infringement of Privacy; Wrongfulness

An infringement of privacy can take place through acquaintance with personal facts by outsiders contrary to the determination and will of the person whose right is infringed. This acquaintance can take place through intrusion (or acquaintance with private facts) and disclosure (or revelation of private facts) and disclosure (or revelation of private facts). Neethling²⁹ submits that the wrongfulness of an infringement of privacy should *mutatis mutandis* be judged in the manner as that of conduct infringing dignity and that of conduct as a result, the acquaintance with private facts should be not only contrary to the subjective determination and will of the prejudiced party, but at the same time viewed objectively, contrary to the views of the community or unreasonableness.

²⁷ *High Court in Park-Ross v Director Office for Serious Economic Offences* 1995 (2) BCLR 198 (C)

²⁸ See *Katz v United States* 389 US 347 (1967)

²⁹ Neethling (refer note 6 above) 243

2.10 Intrusion or acquaintance

Neethling³⁰ distinguishes between two types of intrusion namely acquaintance with private facts (where such acquaintance is totally excluded or is limited to specific person) and secondly (where acquaintance is permissible to an indeterminate but limited number of persons).

- (i) Private facts totally excluded or limited to specific persons

An acquaintance with one's private facts may be regarded as an infringement of the right to privacy, simply because not every person has access to those facts. There is an element of confidentiality and hence acquaintance with them is contrary to the determination and wishes of the holder of the right as well as being in conflict with the opinion of the community and thus wrongful.

- (ii) Private facts available to indeterminate but limited number of persons

Acquaintance with personal facts available to an indeterminate but limited number of persons is in principle not wrongful unless the acquisition is contrary to the dictates of human nature and the composition of modern society. The circumstances of each case will dictate whether an intrusion is wrongful or not.

2.11 Disclosure or revelation

The infringement of privacy through an act of disclosure comes about where there is revelation of plaintiffs personal and private facts to third party by outsiders,

³⁰ Ibid 243

which although known to the outsider nonetheless remains private. Neethling³¹ distinguishes three types of disclosure and submits that in all of them the question of infringement of privacy arises only if the plaintiff is identified with the disclosed facts. The disclosures identified are as follows:

(i) Private facts acquired through wrongful intrusion

Acquisition of private facts through a wrongful act of intrusion and a disclosure of those facts constitute an infringement of the right to privacy. In the judgement of *Motor Industry Fund Administrators (Pty) Ltd v Janit*³² where the Court had to decide whether the respondents were entitled to use information on tape recordings which had been stolen from the applicants by a third party in civil litigation between the parties. The Judge was of the opinion that a court in civil proceedings should have a discretion to exclude even relevant information as admissible evidence. The findings were motivated as follows:

modern technology enables a litigant to obtain access to the most private and confidential discussions of his opponent; his telephones can be tapped, a listening device can be planted in the boardroom (or bedroom) of the opponent, documents can be Photostatted, tape recordings of meetings stolen.....It is poor solace to the litigant whose privacy has unlawfully been invaded by those means that the perpetrator of the wrong may face criminal prosecution if the evidence so obtained can be used in the civil proceedings in which they are engaged. In my view, as a matter of public policy, a court should have a discretion to exclude evidence which was unlawfully obtained.

³¹ Ibid 248

Similarly, it is unacceptable to summarily disregard all evidence wrongfully or illegally obtained. The circumstances of each case should determine how a court should exercise its discretion.

(ii) Confidential relationships

According to Neethling³³ the wrongfulness of conduct becomes problematic where only some specific individuals are privy to private facts in accordance with the determination and will of the plaintiff and consciously disclose the facts either to a single person or a small group of persons as opposed to mass publication. This may not be contrary to convictions of the community since disclosure is harmless and in accordance with human nature. A confidential relationship worthy of protection does not arise only come about when a person is compelled to disclose personal facts to another; it also comes about where there is agreement between the parties that private facts disclosed will be confidential or secret and in such instances disclosure of the private facts involved, apart from breach of contract, will also constitute an infringement of the right to privacy³⁴.

(iii) Mass publication

Neethling³⁵ maintains that with regard to mass publication, that is, disclosure to an unlimited number of persons of facts intended to be accessible to specific persons only, the publication thereof will in principle infringe the right to privacy. This is more so because these facts are characterised by an element of confidentiality. It

³² *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W)

³³ Neethling (refer note 6 above) 249

³⁴ *Ibid* 249

³⁵ *Ibid* 254

has been recognised that the right to privacy is an independent personality right, therefore it can be accepted that in future the mass publication of private facts obtained through a wrongful act of intrusion, or that is contrary to a legally recognised confidential relationship, will probably be considered as an infringement of a right to privacy.

In the judgement of *Mhlongo v Bailey*³⁶ the defendant, without the permission of the plaintiff published the latter's photograph in a journal as part of an article on a female singer. In the article it was averred that the plaintiff, who at the time of publication was a school-teacher, and the singer were involved in an amorous relationship. The plaintiff instituted action on the grounds of infringement of his privacy and dignity. The Court held that the plaintiff's *dignitas* had been infringed.

Mass publication of private facts may be regarded as infringing private facts. In the judgment of *National Media Ltd v Bogoshi*³⁷ the Court held that the media will only be afforded protection to the publication of material in which the public has interest. In this case a question arose with respect to the modern approach. In my opinion this seeks to strike a balance between the right to the reputation on the one hand and the freedom of expression on the other. The debate whether the press should be strictly liable for defamatory remarks it publishes was conducted within the parameters of relevant constitutional provisions of the South African Constitution, namely section 15(1), which entrenches press freedom in specific terms.

³⁶ *Mhlongo v Bailey*: 1958 1 SA 370 (W)

³⁷ *National Media Ltd v Bogoshi* 1998(4) SA 1196 (SCA)

It would seem that to hold press strictly liable for alleged defamatory remarks is inappropriate in modern society based on a constitution that entrenches a bill of rights and that guarantees certain rights of the press. Such a law is offensive to modern thinking and ought to be closely scrutinised by the courts.

The preferable view is that a balance needs to be struck between the right to human dignity or reputation and freedom of expression under which freedom of the press is subsumed. But it is one thing to state the necessity to balance the above rights, and a totally different thing to actually do so. Quite often, depending on the orientations of the judges no such balance is attempted, instead a justification in favour of one of the above considerations is mounted. Those who favour the freedom of expression consideration tend to place onerous conditions on the plaintiff who have been recklessly injured by the press. For instance, it has often been said that those who hold public office are expected to have a thick skin because they voluntarily subjected themselves to public scrutiny and that they should be able to accommodate stinging criticism, even if some may be factually misguided. The cardinal issue is that there must not be any malice by the press report. This line of reasoning sometimes over-privileges the freedom of expression over the right to dignity.

In balancing the right to reputation and the freedom of expression there is no need to adopt a rigid approach. The determining criteria in my view should be whether in the circumstances of a particular case was the alleged defamatory statement justifiable in a democratic society. Framed in this manner the courts would be freed from the paralysis of analysis occasioned by treating the old and modern defenses as biblical commandments cast in stone. The courts must develop

guidelines of how to strike a balance between freedom of the press to publish and protection of people's reputations. It is indisputable that no democratic society can permit the press to run vendettas against individuals who are powerless to arrest falsehoods against them being published.

2.12 Justifying a right of employee privacy

Everybody values their privacy and employees are no exception to the rule. Craig³⁸ has identified four justifications for recognizing a personal right of privacy in individuals and they all have force in the employment context. He states that each is premised on the promotion of a distinct social value. The four justifications are; autonomy, dignity and well being, healthy relationship, and pluralism.

(i) Autonomy

Craig³⁹ submits that privacy is often linked to the concept of autonomy, meaning the ability of an individual to choose freely and independently his goals or relations. Employment impacts significantly on an individual autonomy, as the very nature of the employment offers some degree of control and subjects the employee to the interest and objectives of the employer. This does not have to be regarded negatively as since it comes with economic rewards for the employee which promote an individuals autonomy and independence in society.

In addition Craig⁴⁰ states that worker autonomy may be affected in two ways. Firstly a management policy may threaten to penalize candidates/employees for activities occurring outside the workplace which have a small bearing or even none on the relationship to the legitimate management interests. For example, drug testing has

³⁸ Craig Privacy and Employment Law(1999) 20

³⁹ Ibid 21

been criticized because employers may refuse to hire, or may discipline individuals for their use of drugs away from the workplace. Secondly, the problem of employer control over workers' private lives becomes more complex as on-duty and off-duty time blurs. This was captured eloquently by Justice Blackmun in *O'Connor v Ortega*⁴¹ when he stated the following

The reality of work in modern times, whether done by public or private employees, reveals why a public employees' expectation of privacy in the workplace should be carefully safeguarded and not slightly set-aside. It is unfortunately all too true that the workplace has become another home for most working Americans. Many people spend the better part of their days and much more of their evenings at work.....consequently, an employee's private life must intersect with the workplace, for example, when the employee takes advantage of work or lunch break to make personal telephone calls, to attend to personal business, or to receive personal visitors in the office. As a result, the tidy distinctions.....between the workplace and professional affairs, on the one hand, and personal possessions and private activities on the other, do not exist in reality.

Because the employment relationship places a great amount of control over individual autonomy and independence, any management practice which exerts control over the

⁴⁰ Ibid 21

⁴¹ *O'Connor v Ortega* 107 S.Ct. 1492 (1989) 76

private interests of candidates/employees is cause for serious concern and need close attention⁴².

(ii) Dignity and well being

Further more Craig⁴³ states that privacy is not only important because it provides individuals with protection from social pressures for the purpose of autonomous decision making but also because it affords everyone an environment where they can free to be themselves. Individual's state of mind is preserved and promoted by the protection of private life. Denial of privacy may result in some disturbance to an individual normal state of being Management practices implicating private interests may adversely affect the dignity and well being of candidate/employees.

(iii) Healthy Relationships

The employment relationship is crucial to most people and hence employment transcends its contractual nature, and operates as a social relationship based on trust, respect and good faith. Craig⁴⁴ states that one labour group observed that;

It seems trite to say that a happy worker is likely a productive worker that a worker who is accorded respect is likely to return it.....On the other hand, a worker who must produce in an atmosphere of distrust and lack of consideration seems more likely to treat her or his employer in kind.

The issue of privacy has the potential to cause conflict between management and employees, and a relationship that lacks trust is always difficult to manage.

⁴² Craig (refer 38 above) 22

⁴³ Ibid 22

(iv) Pluralism

Craig⁴⁵ believes that privacy often brings about diversity, which is crucial to any pluralistic, democratic society. The importance of pluralism in the privacy of individuals, whether or not in their capacity as workers is a serious matter. Moreover pluralism plays an important role in the workplace, where innovation is so critical to the success of any organisation. Innovation occurs through industrial pluralism –the fostering of new ideas and new approaches.

2.13 Conclusion

The right to privacy like all other rights needs to be protected but it is also subject to limitation as enshrined in section 36 of the Constitution. The important issue is balancing of interest since one must appreciate the fact that where there is interaction with others the right to privacy is bound to shrink accordingly but at the same time people should not be made to feel that they have no control over issues that they consider private just because they have left the domain of their homes. Employees spend a great deal of their time at work and naturally expect some reasonable degree of privacy at work however this may pose a challenge for an employer to enforce his right to manage without being taken to task for invasion of privacy.

⁴⁴ Ibid 24

⁴⁵ Ibid 25

3. MANAGERIAL PREROGATIVE

Management and workers have different views and perceptions regarding the various areas that constitute managerial prerogative. Management regards certain issues as falling within their managerial prerogative and hence not subject to consultation, but over time management has come to realise that good industrial relations requires that there should be consultation between all the stake holders especially dealing with the various mechanisms that an employer may want to introduce regarding discipline at the work place. It is also undeniable that there is bound to be some overlap between the employees privacy and the employers right to manage. It therefore becomes a challenge to strike a balance between the two as succinctly captured by the Victorian Law Reform Commission⁴⁶ as follows:

Workplace privacy raises difficult questions about the appropriate balance to be struck between employer's claim to exercise management and control over workers, and the rights of employees to have their autonomy and privacy respected and to be treated with dignity.

Reinhard⁴⁷ raises the point that the use of technology has added to an already existing competition between the employer and the employee. He states that on the one hand there is the principle of inviolability of the employees private lives and the private communication and on the other, the principle of the employers' rights to enjoy their private property and their managerial rights to enjoy their private property and their managerial powers of command.

⁴⁶ VLRC, *Privacy Law: Options for Reform* (2001) 48

3.1. The term managerial prerogative

The term prerogative denotes a right or privilege, which belongs to a particular group or persons. Barker and Holthausen⁴⁸ define managerial prerogative as;

Those rights reserved to management which it feels are intrinsic to its authority to manage. Management maintains that such rights are not subject to collective bargaining nor do they require consultation with the union.

In the labour relationship employer prerogative entails the right to manage an organisation. It refers to the right to make decisions regarding the aim of the organisation and the ways in which it will achieve these aims. The decisions referred to can be divided into two broad categories, namely the decisions about human resources utilized by the organisation and decisions of an 'economic' or 'business' nature. Decisions about human nature involve deciding on the number and types of employees required, their terms and conditions of employment, where and how they do their work and the supervision of their work. Decisions of an 'economic' or 'business' nature include decisions relating to the acquisition and/or use of physical assets needed by the organisation and decisions regarding the aims of the organisation, the products it produces or the services it produces. Managerial prerogative is mostly regarded as being of special importance when dealing with decisions regarding human resources utilized by the organisation. It is linked to the ability of the employer to control the activities of employees in the workplace.

⁴⁷ Reinhard H *Comparative Labour Law & Policy Journal: Information Technology and Workers Privacy*; Enforcement Vol 23 No2 Winter 2002, 527

⁴⁸ F.S. Barker & M.M.E. Holtzhausen *South African Labour Glossary* (1996) 90

In *George v Liberty Life Association of Africa*⁴⁹ the court described the prerogative of an employer as ‘the totality of the capacity of an employer’. This characterisation is with due respect rather vague. Managerial prerogative should strictly speaking be confined to ordering production and other matters incidental thereto.

Jordaan⁵⁰ maintains that if any employer was asked to define the concept of managerial prerogative his answer would likely be that it is has something to do with the right to order production and labour. He states that on one hand the power to order production can probably be explained in terms of the fact that the employer either owns or in some manner controls, industrial capital, that is the material assets employed in the production process. On the other hand the power to command human resources cannot be justified on that basis. While the power to command production rests on ownership or control of industrial capital, contract is the source of managerial control over employees. Ownership or control of industrial capital does not legally give the employer the right or the power to ‘manage’ employees or exercise control over them. The right to manage and control property only extends to the object owned or controlled, but does not include the right to manage or control persons.

3.2 The legal basis for managerial prerogative

There are a number of differing opinions on what constitutes the basis for managerial prerogative. In order for employer prerogative to be legally enforceable it must have its origin in the law. Lawyers find its origin in the contract of employment, which has subordination of the employee to the authority of the employer as one of its elements. This element creates the legal right for an employer to manage the employee as well

⁴⁹ *George v Liberty Life Association of Africa* (1996) 17 ILJ 571 IC, 582

⁵⁰ Barney Jordaan; *Management Prerogative and Industrial Democracy*. (1991) 11 (3) *Industrial Relations of South Africa* 1

as the legal duty on the employee to adhere to the employer's instructions⁵¹. In *Checkers SA Ltd (South Hills Warehouse) & SA Commercial Catering & Allied Workers Union*⁵² the arbitrator explained the concept as follows:

It is true that the parties agree not only to a specified ambit of responsibility, but also to an inevitable degree of subordination. This entails that, within the limits of the employee's degree of subordination he or she is required to submit to the employer's instructions.

This point is further emphasised by Rycroft⁵³ who argues that:

The legal basis for managerial prerogative is generally acknowledged to be the traditional law of master and servant infused into the employment contract. This infusion has allowed the employer to fend off threats by employees to everyday control of the enterprise simply because the employment contract is silent on a particular aspect of the numerous contingencies arising in the course of employment.

It is imperative to note that the contract of employment cannot be separated from the economic and social realities within which it comes into being. The legal foundation for the employer decision-making power is the contract, but this right is reinforced by the employer's greater economic power and social position.

⁵¹ Ibid 3

⁵² *Checkers SA Ltd (South Hills Warehouse) & SA Commercial Catering & Allied Workers Union* 1990 11 ILJ 1357 (ARB)1365 1

⁵³ A Rycroft 'Obstacles to Employment Equity' *The Role of Judges and Arbitrators in the Interpretation of Affirmative Action Policies* (1999) 20 ILJ 1411, 1417

However, as pointed out previously Jordan⁵⁴ does not support the argument and maintains the position that ownership or control of industrial capital does not legally give the employer the right or the power to ‘manage’ employees or exercise control over them. The position undermines the position of power of capital. Capital by definition is more powerful than the individual. Whilst it may be legally correct that ownership of capital does not give the employer the right to employees in actual fact it does because it is the employer who is capable of dismissing the employee and not the other way round.

Flanders⁵⁵ believes that the employers’ prerogative is based on the fact that only its managers have the necessary skills and expertise to manage present-day activities with their large work-forces and advanced technology. The right to manage is derived from the market power of the employer and that no equality of bargaining power in the labour market prevails in an employment relationship as an employer has capital, information and access to legal advice. Strydom⁵⁶ believes that there is some merit in the argument that explains the practical realities of the subordinate position of an employee in an employment relationship, but however these social and economic realities do not confer upon the employer a legal right to manage its employees. The other ground for employer’s prerogative is the bureaucratic organization of an enterprise. When an employee joins an enterprise, he or she forms part of a bureaucratic organisation in which he or she yields little or no bargaining power to those above in the system of ranks. Strydom⁵⁷ is however quick to point out that this ground as a legal basis for managerial prerogative must be rejected as bureaucratic

⁵⁴Jordan (refer 50 above) 2

⁵⁵A Flanders, *Management and Unions, The Theory and Reform of Industrial Relations* 1970, 135

⁵⁶E.M.L. Strydom “The Origin and Nature and Ambit of Employer Prerogative” (part I) *SA Mercantile Law Journal*; Vol 1, Iss (1999) 48

⁵⁷Ibid 48

organisation does not confer a legal duty on the employee to obey instruction from supervisors. It is merely a decision-making structure devised by the employer to exercise the maximum amount of control over the employees.

The arguments as submitted by Strydom make reference to the economic and social realities of the employment relationship. In most instances the relationship is between a bearer of power and someone with little or no bargaining power. The degree to which managerial prerogative exists depends on the power relationship. Those with economic power are able to influence the ones with little or no economic power.

Another factor is the prevalent competition amongst job seekers particularly when the economy is in a downward phase and unemployment is high. These social and economic considerations do not however provide a legal basis for the employer to manage his/her employees, and conversely, for the employees to obey the employers' instructions.

Jordaan⁵⁸ on the other hand maintains that whether management rights are expressed or implied, the right to manage is generally seen as being a cluster of substantive rights. He states that however it has been asserted that right to manage is, in fact, a procedural right:

The right to direct, where it involves wages, hours or working conditions, is a procedural right. It does not imply some right over and above labor's right. It is a recognition of the fact that somebody has to run the plant. People can't be wandering around at loose ends, each deciding what to do next. Management decides what the employee is to do. However this right to direct or to initiate

⁵⁸ Jordaan (refer note 50 above) 1418

action does not imply a second-class role for the union. The union has the right to pursue its role of representing the interest of the employee with the same nature accorded it, as is management. To assure order, there, is a clear procedural line drawn: the company directs and the union grieves when it objects.

3.3. The purpose of managerial prerogative in an establishment

There are a number of reasons or purposes or why management collects personal data on job applicants. According to the ILO⁵⁹, management collects personal data for the following purposes; comply with the law, to assist in selection for employment, training and promotion, to ensure personal safety, personal scrutiny, quality control, customer service and the protection of property.

Strydom⁶⁰ believes that in order for an organisation to fulfill its stakeholders interests there is need to have managerial prerogative to coordinate the skills, effort and activities of its members so as to attain its goals. There has to be some persons, or body of persons, within the organisation charged with the responsibility and authority to steer the organisation towards the attainment of its goal by deciding on the adoption of the best practice to attain the goal and by allocating functions and its duties to members of the organisation and supervise those activities. Those people that have been given the responsibility to execute their power must do so within the limits imposed by the hierarchical structure of the organisation. Managers who act as employer's agents mostly exercise employer's decision-making powers.

⁵⁹ ILO Code of Practice on the Protection of Workers Personal Data ILJ Vol 18 Part 1 1997 (28)

⁶⁰ Strydom (refer note 56 above) 43

3.4 The scope of employer prerogative

It has already been stated that both the union and management agree that the employer/ management has the right to manage. However there are differing perspectives on the scope of the employer to manage. Strydom⁶¹ has broken them down as follows:

3.4.1 An industrial relations perspective on the scope of employer prerogative

Industrial relations is commonly regarded as an amalgamation of different interest groups such as the employees and their trade unions, shareholders and consumers, presided over by a top management which serves the long terms needs of the organisation by paying due concern to all these different interests⁶². There is an acceptance that the employer has the decision-making power pertaining to the economic or business component of the business such as policy issues, and the goodwill of the organization, however the employer's prerogative regarding the employees must be restricted. There has to be an obligation on the part of the employer to negotiate or bargain with the trade union about matters that fall within the 'job territory' or immediate work environment of employees.

Filho⁶³ emphasizes that it is not always easy to balance the rights and interest of employers and employees but however notice and consent may constitute important

⁶¹ Ibid 50

⁶² Ibid 50

⁶³ Filho R F & Jeffrey M *Comparative Labour Law & Policy Journal*; 'Information Technology and Workers Privacy: Notice and Consent' Vol 23, No2 Winter 2002, 566

factors to be taken into consideration and may have an important influence upon the outcome. This however does not imply that these are the only issues to be considered but they merely provide us with useful information and guidelines.

It is trite to note that industrial relations authors in addition to collective bargaining also regard the law as a factor that must limit or restrict the employer's prerogative. Strydom⁶⁴ defines employer prerogative as:

The residue of discriminatory powers of decision left to management when the regulation impacts of law and collective bargaining have been subtracted.

Flanders⁶⁵ on the other hand states that it is not only collective bargaining and the law that restricts the employer's prerogative but also control by market forces and accountability. Market control relates to the availability of work, which, in turn depends mainly on the economy. Employer prerogative is at its strongest when the economy is at its weakest, as a weak economy results in job scarcity and a large potential workforce for employers to choose from.

3.4.2 Employers perspective on the scope of their prerogative

Bendix⁶⁶ believes that a majority of employers when first confronted with trade unions and their demands felt that their prerogative should not be restricted in any way. To support their position they adopted a unitary perspective of industrial relations. Their arguments were that every enterprise was an integrated and harmonious entity that existed for a common purpose. The proponents of this view assumed that every employee identified with the aims of the organization. They

⁶⁴ Strydom (refer note 56 above) 52

⁶⁵ Flanders (refer note 55 above) 136

believed that there could be no conflict between the interests of the employers and the employees. The employers and the employees were all striving towards the attainment of the organization's goals, profits and pay in which everyone in the organization had a stake.

This unitary perspective according to Bendix⁶⁷ may not be ideal to the business particularly where there is a strong trade union representation. As a result of the shortcomings associated with the unitary approach most employers have changed to the pluralist view and accepted that certain aspects of the business are of importance to the unionised employees and should therefore be made subject to collective bargaining. Employers however were not too willing to bargain about economic issues as they consider them to be within their exclusive prerogative. They were however willing to bargain about labour-related issues. The change in the legislation has however seen a change into more extensive forms of participation such as negotiation, consultation, joint decision making and the topics for such participation include ones that are regarded as falling within the business sphere of the enterprise.

3.4.3 A Labour Law perspective on the scope of employer prerogative

One of the views held by labour lawyers regarding management is that it has a decisive say in the running of the enterprise and all business and commercial decisions. In *Checkers SA Ltd (South Hills Warehouse) and SA Commercial Catering and Allied Workers Union*⁶⁸ the court stated that

...management has the prerogative to manage. This means as Brassey has pointed out, management has a decisive say over the conduct of the enterprise

⁶⁶ Bendix S *Industrial Relations in the New South Africa* (1996) 603

⁶⁷ *Ibid* 603

and over all business commercial decisions. Arising from this, in the second place is management prerogative to impose reasonable and fair disciplinary regulation upon its workforce. Firstly management has been subjected to an obligation to enter into negotiations with a representative union. Secondly, the rules laid down or requirements imposed must be both fair and reasonable. But subject to these requirements ...management may take the initiative –and thus exercise the ‘prerogative’ of laying down rules. The third area in which managerial prerogative may come into play is the lawful ambit of employees responsibilities. Here management’s prerogative to act unilaterally is considerably more restricted than in the other two areas.

There has been an important development in labour law in South Africa that has had an important impact on the doctrine of managerial prerogative. The provision of ‘workplace forums’ in the Labour Relations Act is a significant innovation in that the concept it embodies is completely new to our law. One has to recall that South Africa’s legacy of repression and intensively adversarial industrial relation has generally been seen as an obstacle to employment development. The provision for work-place forum represents a shift from the tradition of adversarial collective bargaining on all matters to joint problem solving and participation.

3.5 Workplace Forums

According to Summers C⁶⁹ countries which have prospered both domestically and in world competition are those that have developed institutions and attitudes that have fostered a sense of partnership between management and employees in the running of

⁶⁸ *In Checkers SA Ltd (South Hills Warehouse) and SA Commercial Catering and Allied Workers Union* (1990) 11 ILJ 1357
⁶⁹ (1995) ILJ Vol 16 no 4

the enterprise. Aranda⁷⁰ believes that 'without suitable collective protection, individual rights are of less value'. In the South Africa such partnership is realised through workplace forums. The Labour Relations Act provides that an employer shall consult with a workplace forum with a view of reaching consensus. It provides that where an employer and the workplace forum do not reach consensus in respect of proposals put forward, then an arbitrator should be brought in and he/she should have the final say in such matters. The final decision to execute the proposal rests with management as the employer has the authority in the form of a managerial prerogative over the employee and also the employer, because of his stronger bargaining position can almost unilaterally lay down terms and conditions of service.

The employer must also disclose to the workplace forum all relevant information (subject to some exceptions) that will allow the forum to engage effectively in consultation and joint decision making⁷¹. Some of the matters for consultation are listed in section 84 include among other things restructuring the workplace, including the introduction of new technology and new methods, changes in the organisation of work, partial or total plant closures, mergers and transfers of ownership in so far as they have an impact on the employees, the dismissal of employees for reasons based on operational requirements, and exemption from any collective agreement or any law. For example in Germany employers must inform Works Council, comprehensively and in advance, of any new technical equipment that they intend to introduce, they must provide all the necessary information that the Works Council needs in order to exercise its right of supervision.⁷²

⁷⁰ Aranda J. T. *Comparative Labour Law & Policy Journal: Information Technology and Workers Privacy; Workers' The Role of Worker Representation* Vol 23' No2 Winter 2002, 533

⁷¹ See for example ILO Convention No 135 on Workers Representatives (1971)

⁷² Reinhard H-S *Comparative Labour Law & Policy Journal Information Technology and Workers Privacy: The German Law.* Vol 23 No2 Winter 2002. 384

Some matters for joint decision making are listed in section 86; they are disciplinary codes and procedures, rules relating to the proper regulation of the workplace in so far as they apply to conduct not related to the work performance of employees, and matters designed to protect and advance persons disadvantaged by unfair discrimination. Matters of joint decision making are limited to issues that have a direct bearing on the conditions of service of employees.

The obligation to disclose information reinforces the ability of workplace forums to demand meaningful consultation and joint decision making.⁷³ Employers however do not have to disclose information that is legally privileged or would cause substantial harm to an employee or the employer, or which is private and personal to an employee, because there is a possibility that this could lead to tension within the workforce if privileged information were to be made known.

3.6 Conclusion

The right to manage will always exist in the employment relationship. The different perspectives acknowledge that notwithstanding the various perspectives employees are required to submit to the instructions of the employer. The contract of employment forms the basis of management control and it is that basis that gives management the authority to manage employees fairly. Consequently as labour relations moves from adversarial relationship to joint problem solving and participation management prerogative is bound to shrink considerably. It is no longer the whip of the employer that will take the company to a different level. It is the joint decision making that ensures that the interests of all the stake holders are protected.

4 WORKPLACE DISCIPLINE

It is generally accepted that the employer has the right to maintain and enforce discipline at the workplace. The right has its origin in the common law, more particularly in the contract of employment. The right to discipline is a term which is implied by the law in the contract of employment. This term is also inextricably linked to the employee's duty to obey all lawful and reasonable instructions. If an employer did not have the right to discipline an employee who does not comply with the employer's lawful and reasonable instruction, the right to give instructions would be meaningless.

Regarding the way in which modern technology is changing Filho⁷⁴ observes that,

....the way in which societies are organised becomes increasingly related to information and communication, the use of the computer and the possibilities provided by it, blur the frontier between private and professional worlds, so enabling the workplace to become a space of total disciplinary control

Consistent with the foregoing is Grogan's⁷⁵ view that obedience implies discipline, discipline implies rules and, rules to be effective imply the power to impose sanctions on those who do not abide by. Accordingly he perceives the power to prescribe standards of conduct for the workplace and to initiate disciplinary steps against transgressors as one of the most jealously guarded territories of managers everywhere, forming as it does an integral part of the broader right to manage.

⁷³ (1996) 17 ILJ 804

⁷⁴ Filho R. F & Leonel de Rezende Almin *Comparative Labour Law & Policy Journal*; Information Technology and Workers Privacy; Old and New Paradigms Vol 23 No2 Winter 2002, 571

⁷⁵ Grogan J, *Workplace Law* 2001 (92)

The function of discipline in the employment realm is to ensure that individual employees contribute effectively and efficiently to the common goals of the enterprise. Production and provision of services would be highly impeded if employees were to be allowed to work as and how they please hence it is the employers right and duty to ensure that the employees adhere to reasonable standards of efficiency and conduct.

4.1 The codes guidelines in respect of the employees right to discipline

Modern labour law recognizes that the purpose of disciplinary sanctions is generally regarded as corrective rather than punitive. The Code of Good Practice; Dismissal in Schedule 8 of the Labour Relations Act endorses the concept of corrective or progressive discipline, which regards it as a means for employees to know and understand what standards are required of them. The Code is intended to guide employers on the procedural and substantive requirements for a fair dismissal. It is also intended to guide arbitrators and the labour court whether dismissal is fair.

A key principle of the Code⁷⁶ is that –

Employers and employees should treat one another with mutual respect. A premium is placed on both employment justice and the efficient operation of business. While employees should be protected from arbitrary action, employers are entitled to satisfactory conduct and work performance for their employees.

Employers are entitled to discipline employees in cases of misconduct or repeated offences. This is the essence of a ‘corrective’ or ‘progressive’ approach to discipline

which aims to modify unacceptable behavior through a system of graduated disciplinary measures such as counseling and warnings.

The Code recognizes that for dismissal to be fair it has to be in compliance with the issues of substantive and procedural fairness as captured in items 4 and 7 of schedule 8. The substantive aspects involve contravention of a rule by the employee whilst procedural aspects involve following of clear procedures by the employer.

In any employment relationship some degree of surveillance and of processing personal data is necessary not only for disciplinary but also for day to day management. An employer may need to process a variety of personal data about the employee⁷⁷ such as information in order to assess an individual's suitability for a given job. An employer may also be obliged to possess private information about regarding their pension allocation in case of death.

⁷⁶ Labour Relations Act No, 66, of 1995 Schedule 8 item 1(3)

⁷⁷ See International Labour Office, 10.2 Conditions of Workers Digest: Workers Privacy Part 1: Protection of Personal Data (1991)

5 WORKPLACE DISCIPLINE AND TELEPHONE ABUSE

An employer's main goal is to ensure that he/she runs a sustainable and profitable organization. It is therefore of paramount importance that employees abide by the rule failing which appropriate action will be taken against them. Employers may engage in a number of ways to ensure compliance with its rules and regulation and some of these ways might involve monitoring and interception of telephone communication.

5.1 The Interception and Monitoring Prohibition Act 127 of 1992

The Interception and Monitoring Prohibition Act 127 of 1992 (IMP Act)⁷⁸ purpose is to prohibit the interception and monitoring of telephone conversation or the interception and opening of postal articles unless a detailed prior procedure has been followed⁷⁹. It states its purpose as follows:

[to] prohibit the interception of certain communication and the monitoring of certain conversations or communication; to provide for the interception of postal articles and communications and for the monitoring of conversations or communication in the case of a serious offence of if the security of the Republic is threatened.

Section 2 of the IMP Act provides as follows;

(1)No person shall-

(a) Intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is intended to

⁷⁸ Interception and Monitoring Prohibition Act 127 of 1992

be transmitted by telephone or in any other manner over a telecommunication line; or;

- (b) Intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization

A number of definitions in this section are relevant in the interpretation on this wide and general interpretation

A 'telecommunication line' is extremely widely defined to include

any apparatus, instrument, pole, mast, wire, pipe, pneumatic, or other tube, thing means which is or may be used for or in connection with the sending, conveying or transmitting or receiving of signs, signals, sounds, communication or other information⁸⁰

This definition is sufficiently wide to include the electronic equipment, linking and distribution systems that serve to connect computers to one another.

A 'monitoring device' is defined as

[A]ny instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication.⁸¹

Mischke.⁸² also states that this definition is wide enough to encompass not only tape recorders, but also other electronic equipment that can be used to record a

⁷⁹ See the US electronic Communication Privacy Act (ECPA) which prohibits the interception and monitoring of electronic communication

⁸⁰ Mischke C; *CLL* Vol 10 No10 May 2001. 93

⁸¹ *Ibid* 48

⁸² *Ibid* 48

conversation or communication, for example a computer can be used to store electronic mail messages. He maintains that the prohibition contained in section 2(1) of IMP Act relates to 'no person' and that the term is not defined in any manner and can therefore be given its ordinary meaning to include, therefore, an employee (whether a natural or juristic person) or a representative of the employee.

Permission to monitor can be given by a judge, who must be convinced that a serious offence has been or is being or will be committed and cannot be investigated in any other manner.

Van Dokkum⁸³ states that it is doubtful that this Act was ever intended to be used in the civil litigation context. Section 3 (2) of the IMP Act provides that any application to a judge for a directive shall be made by a police officer, or an army officer, or to a member of the intelligence service. He⁸⁴ further states that it would seem to be a clear indication that the IMP Act was intended to be used by only the police or the military, including the intelligence services and is not concerned with the interception or monitoring in the private sphere but is rather concerned with the gathering of evidence by public agencies during the investigation of a crime.

5.2 Admissibility of telephone recordings

There have been a number of cases before the South African courts on the application of section 2 of the IMP Act. The cases relate to admissibility of evidence gathered through an unauthorized interception and monitoring of telephone conversation.

⁸³ Van Dokkum N; Class notes 2002, at 200

⁸⁴ Ibid at 200

In *Goosen v Caroline Frozen Yoghurt Parlour*⁸⁵ (decided under the interim constitution) on the admissibility of illegally obtained recordings the court held that illegally obtained tape recordings were in fact admissible. The court's concern was not how the tapes were obtained but rather on whether the recordings were relevant to the matters at hand. The court quoted Hoffman and Zeffert *The SA Law of Evidence* at that:

the general rule stated by Lord Goddard when giving the evidence of the judicial Committee in *Kurma v R*:

in their Lordships' opinion, the test to be applied in considering whether evidence is admissible is whether it is relevant to the matter in issue. If it is, it is admissible and the court is not concerned with how the evidence was observed.

Only if evidence was obtained under duress or is self incriminatory would the court not admit such evidence. It must be mentioned however that broad reading on the question of admissibility is that admissibility of evidence is in principle determined with reference to its relevance. In determining relevance reference must be made to the potential weight of the evidence. The court also accepted that there would be instances where it would be ideal to apply the Bill of Rights horizontally.

The decision of *Protea Technology Ltd and Another v Wainer and Others*⁸⁶ related to an alleged infringement of a restraint of trade agreement. The employer in support of its case had included transcripts of tape recordings of telephone conversations made by the employee whilst still in the employment of the employer. The conversation indicated that the employee was in a breach of the employment contract on the

⁸⁵ *Goosen v Caroline Frozen Yoghurt Parlour* (1995) 16 ILJ 296 (IC)

⁸⁶ *Protea Technology Ltd and Another v Wainer and Others* 1997 (9) BCLR 1225 (W) AT 1237 D-E

restraint of trade. The recordings had been made clandestinely. The respondent argued that the evidence was inadmissible because it had been obtained in contravention of the IMPAct.

The court considered whether the employers actions constituted breach of privacy and found that the right to privacy can be limited and that the individual must have formed a subjective expectation of privacy and also that society must recognise expectation as reasonable. The court in its consideration of the right to privacy considered that the telephone calls were made during company time from the employer's premises. The employer therefore cannot be said to have breached the right to privacy since an employer has a right to know what an employee does during working hours. It held that Wainwright was not entitled to insist upon the protection of the constitutional right to privacy and that the court can exercise its discretion to admit illegally obtained evidence which was reasonable in an open and democratic society.

In the case of *Allied Workers Union of SA on behalf of Ncube v Northern Crime Security CC*⁸⁷ the employee was dismissed after a disciplinary enquiry for using threatening and abusive language to a manager. Some of the conversations had been tape-recorded. The employees union objected to the admissibility of the recordings in evidence. The Commissioner however found that the recordings were not made in contravention of section 2 (1) of the IMPAct in that they were recordings of conversations directly between the employee and the manager, and so were not interceptions' in the sense intended by the Act. Also the intention of monitoring the calls was not to gather confidential information about the employee but rather to verify the threats that he was alleged to have made. The Commissioner maintained

⁸⁷*Allied Workers Union of SA on behalf of Ncube v Northern Crime Security CC* (1999) 20 ILJ 1954 (CCMA)

that he is entitled to exercise his discretion as to whether or not to accept such evidence in civil proceedings.

In the decision of *Mkhize and Bayhead Cold Storage*⁸⁸ the employer suffered losses of R20 000.00. After trying different types of surveillance such as cameras and undercover agents without any success the employer resorted to using the services of a risk management and surveillance camera as a way of apprehending the culprits. Monitoring of telephones included monitoring of a public telephone, which was situated in the premises of the employer. The public telephone recordings revealed some theft taking place by one of the employees who was subsequently dismissed following a disciplinary hearing in which the tape recordings were used as evidence. The employee challenged the admissibility of the evidence claiming that it contravened section 14 of the Constitution. The Commissioner however held that the evidence was admissible.

There is an element of discretion in the admissibility of evidence acquired in contravention of the IMPAct, as evidenced by a South African Airways arbitration award in which the arbitrator exercised his discretion not to admit relevant evidence acquired in contravention of the IMPAct. He maintains that the reason for the arbitrator exercising his discretion against admitting the evidence included the fact that the employer had no evidence to justify the monitoring and that the employer acted on a mere suspicion of drug trafficking. The company also failed to obtain legal advice on the operation and application of the IMPAct and that no legal alternatives to the monitoring of telephone conversation were considered and hence it would be wrong to condone the actions on the employer(SAA) and its flagrant disregard to the

law by admitting evidence which was obtained illegally without even considering alternative methods of obtaining the evidence.⁸⁹

The different decisions on the admissibility of illegally obtained evidence indicates that the courts can exercise its discretion when deciding whether or not to admit the evidence.

5.3 Common law and admissibility of illegally obtained evidence

The common law has been modified to enable a court to exercise flexibility consistent with justice. It assumes that all evidence however obtained is admissible subject to the court's discretion to exclude it. This is however in contravention with the Constitution. In *Protea Technology Ltd and Another v Wainer and others*⁹⁰ the Court's position was that if the common law is at odds with the Constitution the courts must, if that can realistically be done, develop the common law in such a manner as to promote the spirit, purport and objects of the Bill of Rights. Such development requires the test of admissibility to be formulated differently; any evidence which depends upon the breach of a fundamental Constitutional right can only be admitted if the admission of the evidence is justifiable by the standards laid down in section 36(1) of the Constitution. There has to be a balancing of rights. The interest of uncovering must be along the need to ensure that constitutional rights are not negated or obscured. Privacy is not an absolute right under the Constitution nor could it be in practice.

⁸⁸ *Mkhize and Bayhead Cold Storage* Unreported CCMA award

⁸⁹ *Ibid*, 96

⁹⁰ *Protea Technology Ltd and Another v Wainer and others* (refer 86 above)

The courts should retain the discretion to admit evidence, which was relevant, provided that any fundamental right involved were given its proper weight in determining how to exercise that discretion.

5.4 Constitutional right to privacy and monitoring

Section 14(d) of the Constitution provides that everyone has the right to privacy, which includes the right not to have the privacy of their communication infringed.

*In Moonsamy v The Mailhouse*⁹¹ the Commissioner found that tape recordings recorded by way of interception, listening and recording device that was connected to the employee's telephone in his office at the premises of the employer was clearly an invasion of privacy and therefore an invasion of the employees rights in terms of section 14 (d) of the Constitution. The Commissioner however made the following observation:-

It is extremely difficult to clarify, at least with any degree of precision, the nature of the right to privacy of an employee on the premises of the employer during working hours. *In Katz v US*⁹² the U.S Supreme Court held that the individual is entitled to a reasonable expectation of privacy. This reasonable expectation could only exist when the individual had a subjective expectation of privacy and secondly, the society must recognize the expectation as reasonable. Within the context of the employment relationship, the second requirement is largely determined by the 'operational realities of the workplace'. In *O'Connor v Ortega*⁹³ 480 the same Court found that the operational realities of the workplace may make some employees expectation

⁹¹ *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA)

⁹² *Katz v US* 389 US 347 (1967)

⁹³ *O'Connor v Ortega* 480 US 709 (1987)

of privacy unreasonable, which might be found to be reasonable in other non – employment contexts.

The Commissioner then considered whether the infringement could be justified in accordance with section 36 of the Constitution. He observed that the right to privacy in our Bill of Rights was similar to section 8 of the Canadian Charter which reads as follows; ‘Everyone has the right to be secure against unreasonable searches or seizure’. The Commissioner’s decision that there was an invasion of privacy relied in the decision of *Hunter v Southam Inc*⁹⁴ whereby the Supreme Court of Canada held that section 8 was aimed at protecting, at the very least, the individuals right to privacy, which was ‘the right to be secure against encroachment upon the citizen’s reasonable expectation in a free and democratic society. It was held in the *Hunter v Southam Inc* that this purpose required a means of preventing unjustified searches before they happen, and not of determining, after the facts, whether they ought to have occurred in the first place. That could only be accomplished by a system of prior rather than subsequent authorization. The Commissioner therefore felt that privacy clause should be interpreted to similar effect, given the similarity between it and its Canadian counterpart.

In the decision of *Mkhize and Bayhead Cold Storage*.⁹⁵ the Commissioner when dealing with the issue of privacy held that:

With regard toa public phone on the employees premises - the matter is more complex because there is expectation of privacy when using a public telephonea balancing is required between the expectation of the user of the telephone that the call will be private and, on the other hand, the reasonableness of that expectation in the light of the public interest.

⁹⁴ *Hunter v Southam Inc* 11 DLR (4th) 641, 652-3

⁹⁵ *Mkhize and Bayhead Cold Storage* (Refer 88) above

5.5 Waiving of rights

The Employment contract implies that an employee is entitled to basic privacy and dignity but nevertheless there are no laws which prevent an employee agreeing as a condition of employment to being searched and monitored. The general principle is to have this explicitly stated in the contract of employment. In agreeing to searches, monitoring or surveillance an employee is expressly waiving certain privacy rights.

Van Dokkum⁹⁶ states that in the absence of an express term, it is difficult to imply that there is agreement by the employee to be searched or monitored simply because it is an implied term that an employee will not steal from the employer. He maintains that an exception to this general principle would be in instances where there was no legitimate expectation of privacy and that legitimacy depends ultimately on the public norms at the time, or the basic norm of the industry concerned such as a diamond manufacturing company where employees are constantly monitored and subjected to spot searches. Absence of an explicit clause in the contract of employment waiving certain privacy right can be regarded as unconstitutional or lawful unless it is clear that the nature of the job is such that there can be no legitimate expectation of privacy on the part of the employee.

McQuoid Mason⁹⁷ states that the mere fact that the parties on a telephone are aware that they must be careful when talking on the telephone cannot be construed as consent to the violation, or waiver of the person's expectation of the right to privacy.

⁹⁶ Class notes 2002

⁹⁷ Mc Quoid – Mason D in Constitutional Law of South Africa Revision – Service 3 1998 18-17

5.6 Issue of company property

There is no dispute that the telephone at the employer's premises belongs to the employer. However if the employer permits employees to utilize his property (telephone) to make private conversation then this may create an expectation on the part on the part of the employee that those conversations are private.

In the decision of the European Court of Human Rights, *Haford v United Kingdom*⁹⁸ it was held that the employee enjoyed privacy with regard to her office and the telephone line in her office because she was given permission to engage in matters unrelated to her work while in her own office.⁹⁹

In the decision of *Moonsamy v The Mailhouse*¹⁰⁰ the Commissioner stated that it is arguable that even though telephone conversation took place on the employer's telephone (as regards ownership) an employee however expected a certain degree of privacy. Based on that the Commissioner held that there was invasion of privacy by the employer

In the decision of *Warren Thomas Griffiths Union v VWSA*¹⁰¹ the applicant was dismissed for willful disobedience relating to the abuse of the company property; namely the telephone. The company had found out that the applicant had excessively used the company telephone to telephone his girlfriend in Cape Town. The applicant was advised to make his telephone calls within reason and keep costs them at an acceptable level. The applicant did not adhere to the issue of telephone rules but instead he started making his telephone calls from other employees' extensions. The

⁹⁸ *Haford v United Kingdom* (1997) IRLR 47 (ECHR)

⁹⁹ Craig J. DR.; *Privacy and Employment Law* 1999;17

applicant's defense was that the company had no telephone policy and therefore he had no indication of what could be regarded as an acceptable level. The company had decided to dismiss him after there was no significant decrease in the usages of the company telephone. The Commissioner held that the dismissal was fair in that the applicant had been warned not to abuse the company property and that regardless of the fact that there was no policy the amount of time and money spent on the phone was totally unacceptable.

In another arbitration award of *Antonette Dorfling Union v Precision Sharpening Services CC*¹⁰²- the applicant was dismissed after a third and final warning on the abuse of the company telephone. The respondent's position was that the applicant continued to abuse the company telephone even after the final warning and in addition the applicant's performance was greatly affected. The Commissioner held that the applicant's dismissal was substantively fair but procedurally unfair since the respondent did not follow the right procedure.

Craig¹⁰³ states that privacy is a personal right as opposed to a right in property and therefore can be premised on an individual's expectation of privacy, hence it is possible for an employee to have a private interest of a territorial nature within a place in which he possesses no property right. He states that telephone calls may only be monitored to the extent necessary to guard against authorized use of the telephone or to determine the nature of the call but once it is ascertained that the call is personal the employer must cease the monitoring.

¹⁰⁰ Moonsamy v Mailhouse (refer 91 above)

¹⁰¹ Warren Thomas Griffiths Union v VWSA unpublished CCMA case no KN EC 16174

5.7 Issue of company time

An employer has interest in knowing what an employee does during working time due to the nature of the employment relationship. An employer is entitled to request an employee to account for his actions during working hours since an employer expects most of the time to be dedicated towards advancing the interests of the employer and not the employee's. An employer may not compel an employee to disclose the nature of private calls made.

In *Protea Technology Ltd and Another v Wainer and Others*¹⁰⁴ the Court held that an employer could expect the employee to account for his or her activities during the employer's time. The Court stated as follows;

The content of conversation involving the employer's affairs (whether directly or indirectly) is a different matter. The employer is entitled to demand and obtain from an employee as full an account as the latter is capable of furnishing. In this sense also, the company can fairly be regarded as the owner of the knowledge in the employee's mind.

In the same *Protea*¹⁰⁵ decision the Commissioner held that

In reality it is extremely difficult to clarify with any decision of precision, the nature of the right to privacy of an employee on the premises of the employer during working hours.

¹⁰² *Antonette Dorfling Union v Precision Sharpening Services CC* unpublished CCMA case no KN 15866

¹⁰³ Craig (refer note 101 above) 32

¹⁰⁴ *Protea Technology Ltd and Another v Wainer and Others* (Refer 88 above) 1240 B-C

¹⁰⁵ *Ibid* para 74

In an unpublished decision of *Frances Hasessan Jones v Eccles Associates*¹⁰⁶ the applicant was dismissed after being warned to stop spending too much time on the telephone talking to her family. The amount of time spent on the phone affected the applicant's performance. The applicant conceded that the amount of time she spent on the phone indeed affected her work. Numerous counseling sessions were held to try and assist the applicant, but all in vain. The respondent then finally dismissed the applicant. The Commissioner decided that the applicant had been fairly dismissed since the applicant did not reduce time on the telephone discussing personal matters during company time.

5.8 Issue of loyalty and honesty

An employer as stated earlier has a contractual right to know the activities of the employee during working hours. An employer therefore expects an employee to conduct himself in a loyal and faithful manner in executing his functions. In *Moonsamy v The Mailhouse*¹⁰⁷ the Commissioner stated that for this reason alone, and due to the exigencies of the workplace it is clear that the employee's right to privacy at least regarding work related matters must be qualified. However the fundamental issues are how, when and to what extent this privacy should be restricted or limited.

In *Warren Thomas Griffiths Union v VWSA*¹⁰⁸ the applicant demonstrated dishonesty by using other peoples telephone after being warned to reduce the amount of time he spent on the telephone. The employer felt that he had lost trust and faith in the applicant which made the employment relationship difficult.

¹⁰⁶ *Frances Hasessan Jones v Eccles Associates* Case No not stated

¹⁰⁷ *Moonsamy v The Mailhouse* (refer note 91 above)

5.9 Conclusion

It is not controversial that people spend a lot of their time at the workplace and hence there is an overlap between private matters and the employer's working time. The cases referred to however indicate that employer's may not monitor employee's telephone conversations without a reason. In those situations where the employer had to monitor the telecommunications this was normally after an employer had felt that there was a need to monitor the telecommunications. The right to privacy requires that an individual must have formed a subjective expectation of privacy and secondly society must recognise the right as reasonable. There is also evidence that the discretion to admit illegally obtained evidence will always rest with the court but also the discretion must be exercised with regard to the substance of sec 36(1) giving due weight to the need to protect the right which has been breached, policy considerations and the boni mores of the community.

¹⁰⁸ *Warren Thomas Griffiths Union v FWSA* (Refer note 103 above)

6. WORKPLACE DISCIPLINE AND INTERNET ABUSE

There are a number of employment issues that arise out of the use of the computer at the workplace. Employers find themselves faced with the challenge of potential liability for internet abuse against the employees right to privacy. Lack of proper monitoring of the usage of the internet and e-mail by employer may result in lost productivity, degradation of available computing resources and the risk of legal liability. The employer is also faced with the challenge of the degree in which an employee communication may be monitored given the fact that the computer is the property of the employer. An internet User Policy if adopted by the company may assist the control of the use of the computers as well as the sanctions that may be imposed on the employees for the abuse.

Aranda¹⁰⁹ believes that it true that an employer has always had power over employees but compared to traditional monitoring , computer monitoring represents a quantum leap. He states as follows;

We faced with a monitoring that is distant, cold, incisive, constant, surreptitious, and apparently infallible. Never have employers been able to monitor so much and for so long.

6.1 An Internet User Policy

Employers should have an internet user policy which will regulate the use of the internet. The policy must provide for an acknowledgement by the employee that the company's internet system is neither confidential nor private and may be monitored.

¹⁰⁹ Aranda J T, *Comparative Labour Law & Policy Journal*; Information Technology and Workers Privacy; Workers' Privacy: The Spanish Law Vol 23 No2 Winter 2002, 422

The contents of such communication may also be assessed by the company and its employees from time to time for legitimate and lawful business activities. Some of the issues that should be monitored in an internet user policy include prohibition against using the facilities for activities unrelated to the general activities of the company such as the transmission of obscene or threatening material, the transmission of unauthorised distribution of company data and information, removing hardware or software belonging to the firm from the premises without prior written approval, disseminating confidential information and downloading software without reasonable virus protection. Adoption of office policy will set out the rights and obligations of the employer as well as what is expected of the employees and the disciplinary action that can be taken in case of non compliance.

Johnson¹¹⁰ states that although the contents of an internet user policy will vary according to the individual needs of each business the following provisions will be commonplace:

- (i) Rules relating to obscenity, profanity and defamatory language
- (ii) Informing employees about the employer's potential liability for their electronic communication
- (iii) Rules with respect to record retention as well as what information is to be gathered and stored
- (iv) Reasonable guidelines in the scope of monitoring; and
- (v) Rules relating to the use of the internet and e-mail facilities at the office

6.2 Employee Privacy and the Internet Usage

The Regulation of Interception of Communication and Provisions of Communication-related Information Act¹¹¹ came into operation on 30 December 2002 and has provoked a debate whether an employer is permitted to monitor his employees use of his e-mail and Internet facilities. Section 2 of the Act contains a general prohibition from intentionally intercepting or attempting to intercept any communication if one of the parties to the communication has not given prior consent in writing to such interception. This section read with section 2, therefore provides that a third party is prohibited from intercepting, monitoring or recording e-mail and internet abuse (both the content as well as the destination address), without the written consent of one of the parties to the communication¹¹². It would seem that one of the way in which employers can meet these legal requirements is for written consent to be obtained at time of entering into the contract of employment.

Section 6 deals specifically with employee e-mail and internet usage. It states that any “person may, in the course of the carrying 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, in the course of its transmission over a telecommunication system’. A direct communication is defined to include oral communication. An “indirect communication” means the transfer of information, including a message or any part of a message, whether (a) in the form of (i) speech, music or other sounds, (ii) data, (iii) text, (iv) visual images, whether

¹¹⁰ Johnson *J De Rebus*, Nov 2002;55

¹¹¹ The Regulation of Interception of Communication and Provisions of Communication-related Information Act 70 of 2002

¹¹² See also English Law on Regulation of Investigatory Powers Act 2000 Sect 1 which in principle states that interception on public and private systems will not be lawful unless both interlocutors have consented.

animated or not,(v) signals; or (vi) radio frequency spectrum; or (b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or by a telecommunication service, which in turn includes the internet.

A person may only intercept an indirect communication: (a) if the interception is effected by, or with the express or implied consent of, the “system controller” that is the CEO or an equivalent officer or any person duly authorised by that officer; (b) for purpose of monitoring or keeping a record of indirect communication (a) in order to establish the existence of facts; (bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; (cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; (c) if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and (d) if the CEO has made all reasonable efforts to inform in advance a person who intends to use the telecommunication system concern, 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.

It may be argued that this section does not deal with the situation where an employer, who suspects an employee of downloading pornography onto the employer’s business computer, accesses the employee’s computer and then discovers such content on the computers’ hard disk. The section imposes conditions that must be complied with before interception, monitoring or recording can be done, of which the most important is that the CEO must have warned the employees that their e-mail and internet usage will and/or can be monitored to ensure that they do not abuse the employer’s e-mail

and internet policy or the employees prior written consent must have been obtained. The employees implied consent will have been obtained where the employee has to 'accept' certain terms and conditions before he is permitted to use his employer's internet facilities

It seems section 2 and 5 regulate general interceptions, monitoring and recordings of e-mail and internet usage whilst sec 6 regulates specific interceptions monitoring and recordings. A consequence of this is that an employer may intercept, monitor or record e-mail and internet usage in transit, which refers to both the content of the communication as well as the web site address or e-mail address which the employee uses either for sending or retrieving information, provided that the above requirements of sec 6 are complied with.

When the communication reaches the intended receipt, sec 6 no longer play any role in that the communication is no longer "in transit". It can be argued that where an employee returns to his office after working hours, say for example on a Sunday to use his employer's internet or e-mail facilities or e-mail facilities for conduct contrary to the e-mail or internet policy, sec 6 does not govern the scenario in that he did use these facilities during the course of business. Sec 2 and 5 will govern this situation and therefore the employees written consent is required.

6.3 Reasons for monitoring the internet

There are a number of reasons why an employer may wish to monitor the internet, some of the reasons are discussed below.

6.3.1 Company time

An employer expects employees to carry out the company's business during working time after all that is the basis of the employment relationship. An employee who spends most of his time surfing the net instead of carrying out the company's business stands to be disciplined for misusing the employer's time whilst being paid for it¹¹³. In the decision of *Bamford & Others/ Energizer (SA) Ltd*¹¹⁴ employees were dismissed after being charged for abuse of the e-mail. The employer sent out an e-mail instructing all employees to refrain from on-sending ludicrous chain e-mails on company system and company time. The employees however ignored the instruction and were subsequently dismissed for abusing company time. The Commissioner ruled that the dismissal was substantively and procedurally fair.

Paterson¹¹⁵ however states that on the other hand the opportunity for some personal use of the internet may in fact enhance an employee's skills in the effective use of the electronic medium and reduce the amount of time required for personal, face to face transaction. She maintains that a more logical approach is to monitor employees' productive output rather than their electronic transaction and to confine surveillance to situations where there is reason to believe that this may be implicated in a low or reduced level of productivity.

¹¹³ A 1999 survey indicated that a third of employees spend time surfing the Net while at work; another survey that year found that the number of at work visitors to financial web sites increased 37 percent (from 5.95 million to 8.15 million) from December to March 1999. See Finkin M *Comparative Labour Law & Policy Journal*; Information Technology and Workers Privacy; The United States Law Vol 23 No2 Winter 2002, 474

¹¹⁴ *Bamford & Others/ Energizer (SA) Ltd* (2001) 12 BALR 1251

6.3.2 Clogging the corporate network

The internet is the property of the employer and hence should be used as such. Each time an employee uses the internet for a private purpose he or she should know that it he or she is taking up the employer's space on the bandwidth intended for business. For example when one sends an e-mail it goes from the personal computer onto the mail server and then goes into the world wide web until it reaches the mail recipient. The problem is that the medium conveying messages to and on the world wide web has limited space or bandwidth and can get clogged or backed up due to over subscription. If the carriage medium gets clogged because all the space has been taken up then all the information that is transmitted has to wait in line until there is some space. This therefore means the employer business gets slowed down due to the competition of private business of conducted by employees during working hours.

In the decision of *Bamford & Others/ Energiser SA Ltd*¹¹⁶ the employees were dismissed after the employer found that there was a great deal of internet abuse. There was a complaint by some employees that their computer system was inefficient. An audit was carried out which revealed that some of the complainants spend a great deal of time sending out chain letters and pornographic material. It was also found that there was a volume of material running into thousands of communication which had nothing to do with work since most of it was pornographic in nature. Clogging the company's network results in blockage of access and using computer power needed for corporate activities. The Commissioner stated that objectively speaking the trafficking in chain mail and trafficking in chain mail and in pornography was damaging to the business of the respondents and that the most obvious damage was in clogging up the system and running up costs.

¹¹⁶ Paterson M University of Tasmania: Law Review Vol 21 No1 2002:1(2)

Paterson¹¹⁷ however believes that there is a way to addressing clogging of the network. He believes that it would make more sense to tackle the issue of congestion specifically such as identification of peak periods and to request employees to confine their activities to those that are strictly necessary. Another way would be through imposition of technological constraints like limiting the size of attachments that employees could receive. Paterson¹¹⁸ however points out that surveillance could be justifiable in situations where an employee is utilising large volumes of bandwidth during peak times or where their overall internet usage is unusually larger compared to that of their co-workers.

6.3.3 Expressly prohibited use

In South Africa the Provisions of the Films and Publication Act¹¹⁹ prohibits the distribution of child pornography, explicit violent sexual conduct bestiality, explicit sexual conduct which degrades a person and which conducts incitement to cause harm or explicit infliction of extreme violence. The viewing of sexually explicit material in the workplace has a direct impact on fellow employees who are often offended by this material. Employees who therefore engage in viewing sexually prohibited material may be disciplined for viewing material that has been expressly prohibited.

6.3.4 Gender and Racial Issues

If an employee engages in sending material which has gender or racial or sensitive contents it may have serious implications for both the company and the employee who sent the mail. Johnson states that an American Company, Chevron, recently paid

¹¹⁶ *Bamford & Others/ Energiser SA Ltd* (refer note 115 above)

¹¹⁷ Paterson (refer note 117 above) 3

¹¹⁸ *Ibid*, 3

¹¹⁹ South Africa the Provisions of the Films and Publication Act 65 of 1996

\$ 2.2 million in settlement of a sexual harassment claim after an employee posted ‘25 reasons why beer is better than women’ on the company’s bulletin board to which a female employee took exception.

In *Cronje v Toyota Manufacturing*¹²⁰ an employee was dismissed as a result of a racist cartoon distributed at the workplace. The applicant received an e-mail which he printed out to other colleagues at a meeting. The e-mail consisted of a cartoon depicting an adult and a young gorilla, both with the head of President Mugabe of Zimbabwe superimposed on them. The caption stated ‘we want to grow more bananas’. He defended himself by stating that he did not regard the cartoon as racist but rather as a depiction of Zimbabwe as a banana republic. The human resources manager deposed that the respondent’s internet and e-mail usage code specifically outlawed the display and or transmission of any offensive racial, sexual, religious or political images documents on any company system. The factory employed 3500 blacks and 1000 whites, and race related issues were very important on the factory floor. Black employees were upset by the cartoon. The Commissioner found that it was reasonable to include a rule prohibiting the distribution of racist and inflammatory or offensive material in the company’s code. The applicant was aware of the rule which was consistently applied. The Commissioner found the dismissal to be fair.

6.3.5 Vicarious Liability

According to Mischke¹²¹ it is a principle of our common law that an employer may be held jointly and severally liable with an employee for an employee’s wrongful acts

¹²⁰ *Cronje v Toyota Manufacturing* (2001) 22 ILJ 735 (CCMA)

¹²¹ Mischke (refer note 88 above) 46

committed in the course and within the scope of the employees' duties. The issue is clearly captured by Rycroft¹²² when he states as follows:

The employer may not be able to escape liability merely because the act was intentional, amounted to criminal conduct or was specifically prohibited by the employer.

Paterson¹²³ states that activities that may create legal liability include the downloading or distribution of copyright material, the posting of defamatory material on bulletin boards, the circulation of defamatory material on bulletin boards. To substantiate his position he refers to a case in which a Chevron Corporation that paid out \$2.12 million to settle a sexual harassment case brought by female employees as a result of an email titled 'why beer is better than women'.

An employer stands to be held liable for wrongful activities committed by employees¹²⁴ internet and network related acts committed by the employee regardless of the fact that an employer had specifically prohibited those acts. An issue that begs to be dealt with is whether an employee acted within the scope of his or her duties.

Basson¹²⁵ states the following as issues that should be considered in order to constitute employer's liability;

- a) there must be a contract of service between the employee and the employer at the time the employee carries out an unlawful act
- b) the conduct of the employee must have been unlawful; that is the requirements for a delict must be met
- c) the employee must have acted in the course and scope of the employees duties or service. An issue that always poses a challenge in its conviction

¹²² Rycroft & Jordan A Guide to S.A Labour Law 2 ed (1992) 86

¹²³ Paterson M (refer note 115 above) 4

It is therefore imperative that an employer ensures that employees do not engage in activities that may result in vicarious liability through company codes and procedures.

6.3.6 Performance Monitoring

According to Paterson¹²⁶ surveillance of usage of the e-mail and internet usage serves the purpose of monitoring performance as well as enhancing productivity. She states that such commonly used software programme will not only monitor the usage of the internet and e-mail but also has the ability to record every stroke programme used and file opened or copied and to incorporate such information into a searchable report.

6.3.7 Property of the employer

There is no question that in an employment relationship the computer would be the property of the employer. The employer may therefore wish to monitor the internet use such as the size of the message, attachments, the frequency and volume of e-mail sent by an employee, web-sites often visited by the employee and the frequency of hits of those. The regulation of Interception of Communication related Information Act as already mentioned clearly states that there is a general prohibition from intercepting, monitoring or recording e-mail and internet abuse (both the content and the destination) without the written consent of one of the parties to the communication.

An employee would be allowed to make use of the company property to conduct his own personal business but the employer by virtue of the fact that he owns the property would want to make sure that his property is not abused but rather utilised to the

¹²⁴ St Q Skeen *A Criminal Law LAWSA* vol 6 (1996) 378

¹²⁵ Basson et al *Essential Labour Law* (vol1) Individual Labour Law (1998) 50

benefit of the company. It is however imperative that an employer seeks consent of the employees before he/she can introduce monitoring of such communication.

6.3.8 Personal use

Working people spend a great deal of their working time at the workplace. They therefore expect some kind of privacy at the workplace even though they are utilising the company's property. The big challenge is to what extent can an employer permit personal use (that is non-company related use) of e-mail facilities and other communication facilities by its employees. Buys¹²⁷ states that there are those who hold the view that if all personal use is totally prohibited then no employee would have any possible expectation in any stored material (for example computer or e-mail). He however believes that the better practice is to permit restricted personal use of e-mail either internally or externally and then incorporate other policies such as privacy expectation, misuse of company resources around this pragmatic acknowledgement. Personal use should entail some articulated constraints on such use. It should not be allowed to consume a significant amount of the employees workday.

6.4 Conclusion

Computers, computer network have become inextricably linked to our day to day working activities. The employees would have to exercise caution in how they wish to exercise their right to privacy. Failure to observe the employer's policy would result in disciplinary action. It would appear that in a situation where an employee disregards the company's policy then the employees cannot state that the right to

¹²⁶ Paterson M (refer note 115 above)

¹²⁷ Buys R; *The Law of the Internet in South Africa*; (200) at 197

privacy has been infringed since there is no right that is absolute. The employer on the other side would be advised to seek appropriate professional advice and introduce a well drafted internet user policy which reflects the values of the employer, protects the employer's legitimate proprietary interests and respects the reasonable and legitimate expectation of employees to privacy.

7 WORKPLACE DISCIPLINE AND ELECTRONIC SURVEILLANCE

The rise of electronic surveillance is a new concept that is gaining momentum as a result of modern technology in the business circles. For example there is no need to serve a customer over the counter, emphasis is now on self service and only seeking shop attendant's assistance when making payment. It is however imperatives to notify employee why there has to be introduction before embarking in the exercise. Vigneax¹²⁸ states that most national and international norms on workplace surveillance or data processing specifically require the prior notification of the subject; without it these norms deem any such actions to be unlawful²⁹.

Sempill¹³⁰ believes that the issue of workplace surveillance as an issue of public concern is partly because of its centrality in industrial disputes. He states that in New South Wales, a series of disputes between Frankins, a major grocery retailer and the National Union of Workers (NUW), briefly pushed the issue into the print media. The result of that was consideration in the legislative agenda which resulted in NSW'S Workplace Video Surveillance Act¹³¹ – The first and only workplace – specific, electronic Surveillance legislation in Australia.

He maintains that electronic workplace surveillance usually involves private employees who use their superior position to intrude upon and control employees. He believes that workplace surveillance is simply a new albeit particularly offensive, method of enforcing the employer's legal right to secure obedience.

¹²⁸ Vigneax *Comparative Labour Law & Policy Journal: Information Technology and Workers Privacy; Workers' Privacy: Regulatory Techniques* Vol 23' No2 Winter 2002, 512

¹²⁹ See for example Article L. 121-8 of the *French Labour Law Code*

¹³⁰ J Sempill 'Under the Lens: Electronic Workplace Surveillance (2001) 14 *Australian Journal of Labour Law*. 111, 113

¹³¹ NSW'S Workplace Video Surveillance Act 1998

According to Vigneax¹³² the balance of rights requires a balance to be set between two opposing rights: on the one hand the right of employers to check on the work that is being done for them by their employees and, on the other, the right to the employees to some degree of privacy as clearly spelt out in Article 20.3 of the Workers' Statute in Spain, in which an employer may:

[A]dopt the measures of surveillance and control that he sees fit in order to ensure that workers fulfil their contractual obligations and duties, paying due respect in the adoption and implementation of such measures to the human dignity of the workers.

7.1 The implied duty of mutual trust and confidence.

According to Sempill¹³³ in England there is an implied term in all contract of employment to the effect that an employer will not without reasonable and proper cause conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between an employer and an employee. He states that the application – of the implied duty to aspect of employment law involves difficult questions of fact and degree and the issue of workplace surveillance is no exception.

He states that McCallum and McCurry suggest that the implied duty of trust and confidence might limit 'convert observation of changing rooms. They gave a hypothetical scenario whereby a strong case might be made against a male employer who for an improper purpose, installed and operated covert surveillance in a changeroom set aside for female employees. He goes on further to state that if

¹³² Vigneax (refer note 128 above) 505

however some of the factors in this scenario are altered the difficulty of applying the implied term becomes clear. What if the employees are male? What if the surveillance was overt? What if it was authorized by an express term in contract of employment? What if the employer had no compelling rationale for the surveillance, but there was no evidence of an improper purpose? What if there was evidence that drugs were being sold and consumed in the change rooms? What if several employees had requested the surveillance because of the concerns about drug case.¹³⁴

He also believes that the reason why Mr McCallum and Mr McCarry used the changeroom example is because it involves a situation where employees have a high expectation of privacy which is clearly open to employer abuse. He states that in practice many other common electronic surveillance practices may lack the impropriety or 'extreme and deliberate conduct' which is the requirement of the implied duty of trust and confidence. He gives the following examples;

- (a) Employees in the airline and retail industries could argue that covert and overt video surveillance is justified in areas where theft is believed to have occurred, or where there is high risk of theft.
- (b) Employees in the call centre industry could justify audio monitoring by reference to its training benefits and the need for quality control.
- (c) Employees in a range of white-collar professions could attempt to justify e-mail surveillance on the basis that it enables the detection of sexual harassment by e-mail (a common practice) as well as the misuse of sensitive information by employees.

¹³³ Sempill (refer note 130 above) 128

¹³⁴ Ibid 129

The examples of different forms of surveillance described above constitute common commercial practice with clear business rationale but nevertheless the court tradition reluctance to interfere with managerial prerogative may make them unwilling to regard any of them as an abuse of power.

Sempill¹³⁵ goes on further to state that some forms of electronic monitoring may offend the implied duty of trust and confidence there may be a range of legal and practical reasons why the obligation is unlikely, to offer workers a particularly attractive means of resisting electronic workplace surveillance. He states that Stewart has noted 'litigation in the ordinary courts to assert basic employment rights' would be an undesirable prospect for most employees and even unions, given the unpredictable nature of the common law standards, the costs involved and the difficulty of obtaining legal aid.

In *Tap Wine Trading v Cape Classic Wines*¹³⁶ the judge held that in the Conduct of litigation the use of Civil litigation usage of 'trap' with regard to participant electronic surveillance did not infringe any constitutional rights.

7.2 The role of videotapes as evidence of misconduct.

The admissibility of videotapes in labour disputes forums should not present as much a problem as it does in a criminal trial but nevertheless it can raise substantial problem in the law of Evidence since although the onus in civil cases is a less rigorous one, the admissibility of the video tape is a matter of law.

¹³⁵ Sempill (refer note 130 above) 131

¹³⁶ *Tap Wine Trading v Cape Classic Wines* 1999 (4) SA, 194

Landman¹³⁷ observes that the advantages of a video tape were summed up by Van Dijkhoorst J in the *Beleke* case. The court said the following:

The video can be a very helpful tool to arrive at the truth. It does not suffer from fading memory as witnesses do. The camera may be selective but so is the witness's recollection, even more so. The best word artist cannot draw his verbal picture as accurately and as clearly as does the cold eye of the camera. The tape retains for the benefit of court not only the words but also the intimations and emphasis of the speaker and the audience.

He states that in *Protea Technology*¹³⁸ it was held that conducting secret surveillance will invariably intrude on the private rights of the employee because it is more likely than not those private and business related aspects will overlap or at least be captured and thereafter be separated. The employer may face criminal charges of *crimen injuria* but it does not seem that this will make the evidence elicited by secret means inadmissible. He believes that the appropriate way to the admission of evidence obtained in a covertness manner is that if a right that is protected by the Bill of Rights has been infringed then the onus has to be on the party that seeks to benefit in any way from the infringement to satisfy the court that the common law provides a limitation to the nature referred to in Section 36(1) of the Constitution.

7.3 Defence of Property

The right to privacy appears not to enjoy a lot of emphasis when dealing with the issue of defence of property. In *UFCW, Local 1400 v Saskatchewan Co-Operative*

¹³⁷ Landman (1999) 9 Contemporary Labour Law 77 p78

¹³⁸ *Protea Technology Ltd and Another v Wainer and Others* (refer note 86 above)

*Association Ltd*¹³⁹, the employer adopted a loss prevention programme which included hidden video cameras in the workplace to monitor activities within the workplace as a means of investigating alleged thefts. The employer had not communicated to the employees that he was going to set up cameras at the workplace. The Court held that there was no breach of privacy tort because part of an employer's function is to investigate and bring to an end any activities which are causing its business losses. This function according to Craig¹⁴⁰ was recognised in Saskatchewan's Privacy Act which permitted limitations of privacy in defence of property.

The right to privacy in relation to defence of property needs to be exercised with caution, this is illustrated specifically in *McCallum and McCarry* in the hypothetical illustration whereby they state that there is a high expectation of privacy in a changeroom. The case laws referred to also indicate that the right to privacy may be limited by the use of surveillance cameras in those situations where an employer may reasonably justify the need to have surveillance cameras in the workplace. If however there is not justification then an employer would not violate employees right to privacy under the guise of managerial prerogative and the right to manage.

7.4 Conclusion

Modern technology makes it imperative that the law must just catch up. It is not possible to personally police employees as a way of guarding one's interests hence the need to come up with other efficient means such as electronic surveillance.

¹³⁹ *UFCW, Local 1400 v Saskatchewan Co-Operative Association Ltd* (1992) 101 Sask. R. 1 (QB)

¹⁴⁰ Craig (1999) p132

Nevertheless management cannot breach privacy under the pretext that it is management prerogative to monitor what employees are doing and how they are doing it. There needs to be reasonable consideration of the issue of mutual trust between employees and employers which is fundamental in an employment relationship.

8 ADMISSIBILITY OF AND POLYGRAPH TESTING AT THE WORKPLACE

According to Christianson¹⁴¹ in America it has been argued that having to take a polygraph test in order to gain or protect employment is clearly an invasion of privacy even if the results are never seen by anybody. Craig¹⁴² had this to say about polygraph testing;

Polygraph and personality testing constitute profound intrusion into the personal zone of privacy. Such tests are directed at the human mind and thought, which are core interests protected by personal privacy.

In the judgement of *Long Beach City Employees Association v Long Beach*¹⁴³, the Court found the practice of subjecting employees to polygraph testing to be an invasion of privacy contrary to the California Constitution, because the questions asked during the test were 'intimate', 'embarrassing' and 'outrageous'. Pooley¹⁴⁴ supports this in the sense that they believe that the use of polygraph testing to detect deception in the workplace or anywhere else must result in unfairness and discrimination.

Christianson¹⁴⁵ also states that the labour court and the CCMA have had to face the challenge of deciding on the admissibility of polygraph testing. In the case of *Mncube v Cash Paymaster Services (Pty) Ltd*¹⁴⁶ and the unreported CCMA arbitration case of *Harmse v Rainbow Farms (Pty) Ltd* are an indication that the labour dispute

¹⁴¹M Christianson 'Truth Lies and Pornography' *CLL* vol 8 no 1 August (1998) 3

¹⁴²Craig (refer note 38 above) 18

¹⁴³*Long Beach City Employees Association v Long Beach* 719 P 2d 660 (cal. SC 1986) 672

¹⁴⁴Pooley S and Tredoux C *ILJ* Vol 22 April 2001 p 824

¹⁴⁵Christianson (refer note above)

resolution bodies are having to assess admissibility and reliability of polygraph tests as did industrial courts more than ten years ago in *Mhlangu v CIM Delta*¹⁴⁷ when adjudicating misconduct in the workplace. In all these cases there was no specific assessment of polygraph tests and procedures nor has there been any satisfactory opinion on the legal admissibility of these tests.

It is however interesting to note that the CCMA and the labour court have arrived at differing rulings regarding usage of polygraph tests at the workplace. In *SACCAWU obo Sydney Fongo v Pick 'n' Pay Supermarket*¹⁴⁸ the Commissioner accepted that polygraph tests are fool-proof whilst in *Mahlangu v CIM Deltak; Gallant v CIM Deltak*¹⁴⁹ it is said the court cannot ignore the preponderance of expert opinion which holds the view that the use of a lie detector machine..... is on scientific psychological and ethical grounds reprehensible. Similarly in *Jacob v Unitrans Engineering (1999) KN21921*¹⁵⁰, the Commissioner said 'it is absurd to assume that a man is guilty purely because he exercises a legitimate right to refuse to submit to a test or answer a questionnaire.

In the case of *D S Sosibo & others and CTM*¹⁵¹ whereby a dismissal was based only on the evidence of a polygraph test the Commissioner came to the following conclusion;

'the results of a polygraph test are simply an indicator of deception. They do not give details of the extent of misconduct which are essential in the assessment of a sanction....The sole reliance by an employer on unspecific

¹⁴⁶ *Mncube v Cash Paymaster Services (Pty) Ltd* (1997) 5 B.L.R. 639 (CCMA)

¹⁴⁷ *Mhlangu v CIM Delta* ILJ Vol 21 Jan 2000 p33

¹⁴⁸ *SACCAWU obo Sydney Fongo v Pick 'n' Pay Supermarket* (2000) 1FS 15555

¹⁴⁹ *Mahlangu v CIM Deltak; Gallant v CIM Deltak* (1986) 7 ILJ 346 (IC)

¹⁵⁰ *Jacob v Unitrans Engineering (1999) KN219.1.*

polygraph results is insufficient to discharge the onus in terms of s 192 of the LRA to prove that the dismissal was fair. To discharge this onus, the test of a balance of probability is used’.

8.1 Conclusion

An employer may in very limited circumstances use polygraph test but most importantly an employer must prove on a balance of probability that an employee is guilty of the alleged misconduct and only then may he use polygraph test as an addition to the confirm evidence obtained by other investigative procedures. It is also interesting to note the different decisions that have been arrived at by the Commissioners regarding the usage of polygraph testing at work. Polygraph testing in my opinion involves substantiating one’s position beyond reasonable doubt and not on a balance of probability as should be the case in employment matters.

¹⁵¹ *D S Sosibo & others and CTM* (2001) 22 ILJ 811(CCMA) P817

9. CONCLUSION

The recently introduced legislation suggests that until now we were unprepared for the legal challenges associated with highly advanced technology. Employers have now no choice but to keep abreast of these changes since they have a direct bearing on their companies, be it in the form of abuse or in the form of vicarious liability. Employees also have to accept that technology makes it easy for an employer to check their productivity without necessarily asking them to account for their time. This imbalance of power is nothing new as the employer has always had power over employees.

Having surveyed the emerging, but as yet undeveloped, literature in this area, it is clear that the right to privacy takes two forms. An invasion of privacy may assume the form of an unlawful intrusion on the personal privacy of another or the unlawful publication of private facts about a person.

From the case law discussed in this dissertation it would appear that the right to privacy is a two stage enquiry. First whether the conduct complained of amounts to an infringement. Second if there has been an infringement, it must be determined whether such infringement is necessary. One thing that emerges clearly is that where an employer did not seek consent of employees before engaging in practices that may be regarded as invasion of privacy then that employer would have to justify why such invasion is necessary.

The courts appear to balance the right to privacy with the public interest in a majority of cases. It also takes into account human dignity in the execution of the right to

discipline. One thing however that still remains unresolved is at what stage can an employee be said to cease having the right to privacy, especially given the fact that we spend a great deal of our time at the workplace. I do not believe that the court is saying that once we leave the domain of our right then it means we no longer cease to exist as individuals with rights. It is however important to note that employers are not under any obligation to allow employees to utilise an employer's property for personal use. Employees are allowed to make use of the property because an employer accepts that employees have private lives which do not disappear just because they are at the workplace.

With respect to workplace disputes it is generally acknowledged that an employer has the right to discipline employees guilty of misconduct. The courts also appear to be vigilant that the right of workers, especially to privacy, are generally protected but not at the expense of the interest of the employer. It is the nature of the employment relationship that the worker should accept that his or her rights are not absolute but are mediated by workplace dynamics, societal interests and other similar considerations.

It is also critical for employers to have policies on workplace privacy to avoid situations where employees will accuse their employers of invading their privacy. The policy will also serve as a guide on instances such as dismissing employees as well as the various actions to be taken into account before such dismissal can take place. It will also guide those employees that may be unaware of the sensitivity of other issues that may be regarded as humorous by one person only to be regarded offensive by

another person. The policy will therefore facilitate transparency regarding what may lead to a dismissal and what may not lead to a dismissal.

The other question that still needs to be addressed is what should be the limits regarding an employer's power to monitor. When can it be said that there is enough monitoring without necessarily 'invading' privacy 'indefinitely'. The constant monitoring may result in some hostility from employees who may not have full appreciation for monitoring. They may view this as lack of trust on the part of the employer.

The Regulation of Interception of Communication and Provisions of Communication-Related Information Act which came into operation on the 30 December 2002 may address some of the challenges that face employers in that there is clarity that employers' need to seek written consent of employees before any kind of interception or monitoring can take place. The Act however does not address the scenario where an employer accesses the employee's computer and discovers unauthorised content. Whether such conduct constitutes an infringement of the employees constitutional as well as common law right to privacy and consequently *crimen iniuria*, where the employer failed to obtain the employee's oral and written consent or failed to inform him in advance of the computer use policy, remains an open question. Because of the many complex and unanswered questions that arise from the Act, the best way is for the employer to obtain the employees oral or written consent or failed to inform him in advance of the computer use policy, remains an open question.

The complexities and unanswered questions that arise out of the Act mean that the best way is for the employer to seek written consent for the purposes of interception. Once the employee has consented, issues of privacy and ambit of the Act falls away entirely. If an employee refuses consent, the employer can withdraw access to the electronic communication system if this does not amount to a unilateral change in the employee's contract of employment