Aspects of South African Law as it applies to corruption in the workplace

ROCHELLE LE ROUX*

ABSTRACT

The modern workplace is often the closest interface that individuals have with one of modern society's greatest malaise: corruption. Job insecurity and the right to privacy, more particularly cyber privacy, are often perceived as forces undermining the prevention of corruption in the workplace. This article explores the means at the disposal of employers and employees to address corruption in the workplace and endeavours to illustrate that there are aspects of South African law that provide a framework within which corruption can be addressed in the workplace.

Introduction[1]

Available research on local and international perceptions[2] of corruption in South Africa has yielded disturbing results.[3] Unfortunately, these perceptions,

* Bluris (UPE) LLB (UPE) LLM (Stellenbosch) Senior Lecturer, Institute of Development and Labour Law, Faculty of Law, University of Cape Town.

1 This note is broadly based on a paper presented by the author at the 16th Annual Labour Law Conference held in Johannesburg on 2-4 July 2003. I am indebted to Professor PJ Schwikkard (University of Cape Town) for her valuable input.

2 It is impossible to measure actual corruption. The best statisticians can do is provide estimates based on the perceptions of the extent of corruption. See L Camerer 'Corruption in South Africa. Results of an expert panel survey' (2001) *ISS Monograph* 65.

3 A survey conducted by the Centre for Security Studies during 2000 indicates that the involvement of government institutions in corruption is perceived to be high, with provincial and local governments being the frontrunners at 33% and 31% respectively. At departmental level, the criminal justice system (Safety and Security, Police, Justice and Correctional Services) is perceived to be amongst the most corrupt in government. However, government officials are not regarded to be the only champions of corruption: 95% of the respondents in the aforementioned survey indicated that they perceive corruption as a serious problem in areas of society other than government. It is therefore not surprising that the respondents suspected that most corruption occurs at the point where private sector contractors interact with government officials, eg during a tender process. International perspectives are equally disturbing. On the 2003 Corruption Perceptions Index (CPI), South Africa ranked 48th out of 133 countries (the 1st perceived as being the least corrupt). While 85 countries were ranked below South Africa, South Africa's individual score has deteriorated compared to 2002 (CPI, 2003). (Incidentally, out of a clean score of 10, Finland scored the highest (9,7)). South Africa scored only 4,4. Bangladesh, ranked last, scored a mere 1,3 out of 10.) The CPI is essentially a survey of surveys and focuses on corruption in the public sector and is prepared by Transparency International, a global non-governmental organisation devoted solely to curbing corruption. The CPI can be accessed via *http://www.transparency.org/surveys/index.html#cpi* accessed on 6 September 2004.

although they often do not reflect fact, shape international investor confidence in ways that will ultimately impact on the state of the national economy.[4]

While corruption is by no means limited to workplaces, employees could be a valuable resource to uncover corruption in any organisation, but fears of dismissal and/or of being branded as a troublemaker often prevent employees from speaking out.[5] In South Africa, this endemic culture of fear is augmented by high unemployment figures.[6] This, coupled with the uncertainties brought about by restructuring and retrenchments, do not create an environment that encourages any employee to risk his or her job for the sake of being the conqueror of corruption. However, the ability and willingness of employees to blow the whistle or to speak out against their colleagues' mischief is but one side of the anti-corruption coin. The truth is that employers, in an effort to eradicate corruption (and other malpractices), often need to have a closer look at the conduct of their employees. It is in this context that workplace privacy becomes an issue, particularly in light of s 14(*d*) of the Constitution of the Republic of South Africa Act 108 of 1996, which provides that everyone has the right not to have the privacy of their communications infringed.

This article explores aspects of South African law as it applies to corruption in the workplace. More particularly this article will:

(*a*) focus on the means, legislative or otherwise, at the disposal of employers and employees to address corruption in the workplace; and

(*b*) consider the extent to which the right to privacy in the workplace complicates the fight against corruption.

It will, however, be difficult to explore the above without a basic understanding of the crime of corruption. This article will, therefore, commence with a brief explanation of the history and current status of this crime. This will be followed by a discussion of whistleblowing, entrapment and curtailment of gifts as means to address corruption in the workplace. Thereafter, privacy in the workplace, with particular emphasis on electronic communications, will be considered.

---

[4] H van Vuuren 'Corruption, perception and foreign direct investment. Counting the cost of the graft' 2002 11(3) *African Security Review* 67 at 72.

[5] J Bowers, J Lewis and J Mitchell *Whistleblowing: The New Law* (1999) 10.

[6] Statistics South Africa in its March 2003 Labour Force Survey estimates the official unemployment rate at 31,2% and indicates that out of 16,8 million economically active people in South Africa 5,3 million are unemployed. See Statistical Release P0210.

The crime of corruption

The crime of corruption was known as bribery in the common law and could basically only be committed by state officials. Corruption in the private sector was not specifically addressed until the passing of the Prevention of Corruption Act 6 of 1958, which created a separate statutory crime that made it an offence to bribe persons who were not necessarily state officials. The subsequent Corruption Act 94 of 1992 expressly repealed the common law crime of bribery as well as the 1958 Act and introduced a new definition of corruption in s 1(1). This definition is couched in fairly broad terms and covers the situation where a person to whom some power has been conferred, or who has been charged with some duty, is either offered or receives a benefit that is not legally due with the purpose of either inducing that person to abuse such power or to reward the person for the abuse of such power.

During April 2002, the Prevention of Corruption Bill, 2002[7] was published. The Bill follows international trends by "unbundling" corruption, in terms of which specific corrupt actions and practices are defined and prohibited.[8] If implemented, the 1992 Act will be repealed, the common law crime of bribery will be reinstated and a number of newly defined statutory offences will be introduced. Apart from creating a general offence[9] for the corrupt giving or acceptance of any gratification as an inducement to do or not to do anything or as a reward for having done or not having done anything, offences relating to, *inter alia*, the conduct of agents[10], the tendering process[11], witnesses[12], auctions[13], and sporting events[14] are provided for. Gratification is defined to include not only something of monetary value, but also incorporeal benefits such as rights, privileges, votes, consent or influence.[15]

Furthermore, the Bill, in keeping with similar legislation in the United States[16], provides for extraterritorial application[17] to cover any gifts given or received outside South Africa. This is to be welcomed. Although difficult to

---

7 B 19-2002. The explanatory summary of the bill was published in GG no 23336 of 18 April 2002.

8 Memorandum on the Objects of the Prevention of Corruption Bill 2002. See op cit (n7).

9 Section 3 and 4.

10 Section 5.

11 Section 7.

12 Section 9.

13 Section 11.

14 Section 14.

15 Section 1(viii).

16 See G Moody-Stuart *Grand Corruption* (1997) 63.

17 Section 21.

prosecute, globalisation and South Africa's need for foreign investment have increased the likelihood of corrupt payments outside South Africa in respect of the awarding of contracts within South Africa. The Bill also criminalizes the failure of a public officer to report a corrupt approach to his or her supervisor as well as the failure by any other person to report a corrupt approach to the nearest police station.[18] It is suggested that this aspect of the Bill is of particular importance in the workplace, as set out in more detail below. The Bill provides a more holistic (and realistic) approach to corruption and will help to establish collective responsibility for the anti-corruption campaign.[19]

Means to address corruption in the workplace

(a) Whistleblowing

The term 'whistleblowing' refers to the raising of the alarm about a malpractice. In some jurisdictions,[20] legislation exists to provide formal protection to 'whistleblowers'. Whistleblowing is of particular significance in the workplace since it is often the first interface that individuals have with corruption.[21]

However, raising the alarm is not always easy. The relationship between employer and employee is essentially one of trust and confidence, and conduct inconsistent with this notion may warrant dismissal. The failure to assist an employer in identifying culprits 'violates this duty and may itself justify dismissal'[22], but speaking out about corrupt activities in the workplace may be perceived as an act of disloyalty and also be regarded as a ground for dismissal or disciplinary action.

---

[18] Section 20. If convicted for this offence, a person may be liable for imprisonment for up to three years, or a fine, or both a fine and imprisonment. See s 20(3).

[19] Apart from the legal definition, authors on corruption have developed their own terminology. 'Survival corruption' or 'petty corruption' refers to demands for small amounts in return for services. For instance, the small amount demanded by a customs official to turn a blind eye to illegal imports or by an airline official to secure a seat on an apparently overbooked plane. See Van Vuuren op cit (n4) at 68. 'Grand corruption' involves the transfer of substantial amounts to government officials, particularly in developing countries to secure a successful bid or tender. Contracts relating to aircraft, ships, arms, telecommunications and industrial and agro-industrial projects are the most susceptible to this. It is estimated that the commissions paid as bribes often represent 10%-20% of the total value of the project. See Moody-Stuart op cit (n15) at 12-5.

[20] Ie Whisteblower Protection Act 1978 (USA) and Public Interest and the Public Interest Disclosure Act 1998 (UK).

[21] L Vickers 'Whistling in the wind: The Public Interest Disclosure Act 1998' (2000) 20(3) *Legal Studies* 428.

[22] Per Cameron JA in *Chauke v Lee Service Centre CC t/a Leeson Motors* (1998) 19 *ILJ* 1441 (LAC) at 1447C-D.

In South Africa, the Protected Disclosures Act 26 of 2000 ('the PDA') specifically provides protection for employees wishing to blow the whistle on corrupt and other malpractices at their place of work. It is closely modelled on the United Kingdom's Public Interest Disclosures Act 1998 and aims to provide for procedures whereby an employee can safely blow the whistle on his or her employer and be protected against victimization for doing so.[23]

The focus of the PDA is not limited to corruption in the workplace. Rather, it endeavours to encourage employees to disclose information regarding unlawful or irregular conduct by employers or other employees in the workplace, including any criminal offence, endangerment of health and safety and conduct damaging to the environment. In the following paragraphs, the general application of the PDA as well as its relevance in the context of corruption will be discussed.

The scope of the PDA

The PDA provides protection for employees in the private and public sectors. The definition of an employee is the same as in the Labour Relations Act 66 of 1995 ('the LRA') and Basic Conditions of Employment Act 75 of 1997 ('the BCEA'). Unlike the LRA and BCEA, the PDA does not include a presumption as to who an employee is, and a person claiming to be an employee may find it more difficult to prove that he or she is an employee. However, in contrast to the position under the BCEA, unpaid volunteer workers are not excluded from the protection of the PDA. In view of reports of corruption and other malpractices in sport, churches and other charity organisations, this is to be welcomed.

The limitation of the protection of the PDA to employees (and volunteers) is one of the shortcomings of the Act. The Act, in its present form, does not protect pensioners, agents and independent contractors who may operate (or operated in the case of pensioners) within the same workplace as employees and may be exposed to the same corrupt practices.

Essentially, the Act revolves around two concepts: *occupational detriment*[24] and *protected disclosure*[25]. Once an employee makes a disclosure that is protected in terms of the Act, he or she may not be subjected to an occupational detriment. A disclosure will only be protected if it relates to any conduct of an *employer* or an *employee* of that *employer*.[26] An

[23] H Rabkin-Naicker 'The Protected Disclosures Act: Challenges for labour law jurisprudence' (2002) 6 *Law, Democracy & Development* 139 at 140.
[24] Defined in s 1.
[25] Defined in s 1.
[26] Section 3.

employee making a disclosure must have reason to believe that the information concerned shows or tends to show that any of the following has been committed, is being committed or is likely to be committed: a criminal offence; failure to comply with any legal obligation to which that person is subject; miscarriage of justice; endangerment of health/safety of an individual; damage to the environment; or unfair discrimination as contemplated in the Promotion of Equality and Prevention of Unfair Discrimination Act (2000).[27]

This exhaustive list of subjects covered by the PDA is similar to that of the United Kingdom legislation. It is, however, not clear whether serious mismanagement is covered by any of these subjects. The employee has a common law duty to act in good faith and to further the employer's business; mismanagement is arguably a breach of this obligation. The category 'failure to comply with a legal obligation' is significant in this regard.[28] There is no South African case law on this issue, but the exact ambit of this term was put to the test in the UK Employment Appeal Tribunal in *Parkins v Sodexho Ltd*.[29] The appeal tribunal held that the phrase includes a breach of the employment contract and is not limited to legal obligations in terms of the common law or legislation. Parkins (the employee) successfully claimed that his disclosure relating to the lack of adequate on-site supervision (a breach of the employment contract) should be regarded as a protected disclosure. In terms of this approach, mismanagement can arguably be regarded as a failure to comply with an employee's duty to further the interests of the employer and disclosures relating to it should be protected.

The requirement that the disclosure must relate to the conduct of the employer or an employee of the employer is not realistic in the context of corruption and represents one of the major shortcomings of the Act. If an employee makes a protected disclosure to the employer about the corrupt activities of a lucrative client, and the employer, rather than antagonize the client, prefers to silence the employee by, for instance, transferring him or her, that employee will not be protected. Should the Prevention of Corruption Bill 2002 become law, any person subjected to a bribery attempt will be obliged to report it to the nearest police station. It is suggested, however, that the inclusion in the PDA of a similar provision dealing with the conduct of persons other than employers and employees – such as clients and agents – will be more effective.[30]

---

[27] Section 3 read with s 1 and 2(1)(a).

[28] See Vickers op cit (n21) at 434-5.

[29] (2002) *IRLR* 109.

[30] In addition to those mentioned above, the Act has other shortcomings, as identified in Issue Paper 20 (2003), published by the South African Law Commission (tasked to recommend possible amendments to the PDA). These include whether whistleblowers should receive

To qualify for protection a disclosure must be in terms of the prescribed procedures.[31] This means that the disclosure must be made to a person designated in the PDA or it must be a general disclosure. The persons designated are, amongst others, a legal adviser, a person whose occupation involves the giving of legal advice, or the employer.[32]

If a disclosure is made in good faith and substantially in accordance with any procedure prescribed, or authorised by the employer or if it is made directly to the employer in instances where there is no such procedure, the disclosure will be protected.[33] Reasonableness is not required.[34] This omission is consistent with the general purpose of whistleblowing legislation and acknowledges the reality that an employee is very often not in a position to investigate whether his or her suspicion is 'reasonable'. Furthermore, it is in the interests of good business practice to promote over-disclosure rather than under-disclosure.[35]

The requirements for making a protected general disclosure are more onerous than those pertaining to a disclosure to one of the persons or bodies identified in the PDA. It may be made to anyone, but protection will only follow if it is *reasonable* to make the disclosure and the employee acts in good faith and can show that he or she will be victimised or that evidence will be destroyed if the disclosure is made to a person identified in the PDA, that no action was taken after a previous (similar) disclosure or that the impropriety is of an exceptionally serious nature.[36]

If the disclosure is protected in terms of the PDA, the employee may not be subjected to any occupational detriment.[37] In other words the employee may

protection against civil liability and criminal prosecution and whether the employer and the person contravening the Act should be subjected to additional penalties and possibly criminal prosecution. The PDA does not currently provide protection to an employee who commits an offence by making a disclosure that would otherwise qualify for protection, such as officials working for the Revenue Services. It is submitted that the Law Commission should also consider the extent to which a whistleblower's identity should be protected in instances where he or she is the only available witness.

[31] Sections 5-8.

[32] Other designated persons include a member of Cabinet or the Executive Council of a province, or bodies such as the Public Protector or the Auditor General or another body or person prescribed in terms of the PDA. See s 8.

[33] Section 6.

[34] Reasonableness is required in the case of a general disclosure or when the disclosure is made to bodies such as the Public Protector or the Auditor General or another body or person prescribed in terms of the PDA. See s 8(1).

[35] J Gobert and M Punch 'Whistleblowers, the public interest and the Public Interest Disclosure Act 1998' (2000) 63(1) *The Modern Law Review* 63(1) 25 at 40. Also see Van Niekerk AJ's comments in *Communication Workers Union v Mobile Telephone Networks (Pty) Ltd* (2003) 24 *ILJ* 1670 (LC) at 1678A.

[36] Section 9.

[37] Section 3.

not be victimised. Examples of occupational detriments listed in the PDA are disciplinary action, suspension, dismissal, harassment, refusal to promote and the refusal to provide a reference to the employee.[38]

An employee subjected to or fearing an occupational detriment may approach any court having jurisdiction, including the Labour Court, for appropriate relief.[39] The PDA further provides that if an employee is dismissed as a result of having made a protected disclosure, the matter should be dealt with as an automatically unfair dismissal in terms of the LRA.[40] Such dismissals attract the maximum compensation that can be awarded in terms of the LRA namely, the equivalent of 24 months' remuneration.[41] All other occupational detriments (short of dismissal) are to be treated as unfair labour practices in terms of the LRA.[42] This means that the dispute must be referred for conciliation, failing which it may be referred to the Labour Court for adjudication.[43] In addition, the employee may also ask to be transferred if the employee reasonably believes that he or she will be adversely affected on account of having made the disclosure.[44]

The PDA and case law

The judgements in *Grieve v Denel (Pty) Ltd*[45] and *Communication Workers Union & another v Mobile Telephone Networks (Pty) Ltd*[46] both dealt with employees who were subjected to an occupational detriment in the form of disciplinary action after allegedly making a protected disclosure to their employers. In *Grieve*, the court came to the assistance of the employee after finding that there was *prima facie* evidence suggesting criminal conduct and a breach of a legal duty on the part of the employer. In *Mobile Telephone Networks*, however, the court was not prepared to assist the employee. In this case, the employee circulated an e-mail to all and sundry alleging that

[38] Section 1.

[39] Section 4(1)(*a*). This may include interdicting the employer from proceeding with disciplinary proceedings or any other occupational detriment.

[40] Section 4(2)(*a*). Also see s 187(1)(*h*) of the LRA.

[41] Section 194(3).

[42] Section 4(2)(*b*). The 2002 amendments to the Labour Relations Act 66 of 1995 (LRA) introduced a new definition of an unfair labour practice that now includes a reference to protected disclosures. Section 186(2) reads as follows:

> '"Unfair labour practice" means any unfair act or omission that arises between an employer and an employee involving an occupational detriment, other than dismissal, in contravention of the Protected Disclosures Act, 2000 (Act 26 of 2000) on account of the employee having made a protected disclosure defined in that Act.'

[43] Other unfair labour practices are normally referred for arbitration after conciliation has failed. See s 191(5)(*a*)(iv).

[44] Section 4(3).

[45] (2003) 24 *ILJ* 551 (LC).

[46] Op cit (n35).

management and employment agencies were in cahoots regarding certain corrupt practices. The employee was subsequently suspended and charged with misconduct related to the unfortunate e-mail. Van Niekerk AJ applied the legislative requirements strictly in refusing relief. Not only did the employee fail to provide any factual support for his allegations, but he failed to comply with the procedure established by the employer for the reporting of exactly the type of allegations made by the employee. Regarding the requirement of good faith, the judge commented as follows:

> 'The disclosure must also be made in good faith. An employee who deliberately sets out to embarrass or harass an employer is not likely to satisfy the requirement of good faith. It does not necessarily follow though that good faith requires proof of the validity of any concerns or suspicions that an employee may have, or even a belief that any wrongdoing has actually occurred.'[47]

In *Grieve*, the employee, soon after submitting a report to his employer concerning certain suspicious practices, was suspended and instructed to attend a disciplinary enquiry. Apart from a charge relating to accessing pornographic material on the Internet, all the other charges related to the disclosure, although he was not specifically charged for making the disclosure. The court rejected the employer's argument that a disciplinary enquiry does not amount to disciplinary action and indicated that the term is wide enough to include a disciplinary enquiry.[48]

More interesting would have been the situation if the employer only proceeded against the employee (Grieve) on the charge relating to the pornographic material and not on any of the other charges. To what extent would the employee have been protected? Vickers suggests that the employee only needs to show that the whistleblowing was a contributing factor.[49] The onus then shifts to the employer who can only escape liability by clear and convincing evidence that the disciplinary steps would have been taken in any event. This approach was endorsed by Van Niekerk AJ in *Mobile Telephone Networks* when he rejected the employer's claim that the detriment must be directly linked to the disclosure and held that it is only necessary to show some link between the making of the disclosure and the occupational detriment.[50] The employee in *Grieve* would therefore in all likelihood have

---

[47] At 1677J-1678A.

[48] 563F. This is consistent with the approach in *Perumal v Minister of Safety & Security* (2001) 22 *ILJ* 1870 (LC), where it was held that the phrase 'disciplinary action' is not restricted to mean 'disciplinary sanction'. In any event, the mere suspension of the employee amounted to an occupational detriment and it is academic in the context of this case whether disciplinary action included an enquiry or not.

[49] Op cit (n21) at 442.

[50] Op cit (n35) at 2677D.

qualified for protection even if he had only been charged in respect of the pornographic material. This is a clear message to employers to be careful not to take disciplinary action as a form of retribution for making a disclosure, even if such action would otherwise have been justified.

The PDA and workplace procedures

How can employers go about using the PDA and other measures to instil an effective anti-corruption culture at the workplace? Section 6 of the PDA provides that a disclosure to the employer, in the absence of a prescribed or authorized procedure, will be a protected disclosure. It is, however, suggested that a culture of responsible whistleblowing will not be encouraged in an environment where no special channels exist and that it is paramount that employers establish such procedures. Section 6(2) of the PDA provides that an employee who, in accordance with a procedure authorised by his or her employer, makes a disclosure to a person other than his or her employer, is deemed to be making the disclosure to his or her employer. This clearly envisages that the employer may 'contract' this function out to a third party.

Whether or not the function is contracted out, and irrespective of the size of the organisation, it is suggested that the authorized/prescribed procedure should revolve around consultation, education, accessibility and feedback.[51] Consultation will promote the integrity of any procedure adopted. It is also suggested that the normal grievance procedure may not be adequate to ensure confidentiality and that a different procedure involving regulators/confidants, removed from the grievance procedure, may be more appropriate. The procedure should be accessible and opportunities to contact the regulators/confidants away from the workplace by, for example, supplying home phone numbers, should be provided. The PDA does not prohibit anonymous disclosures, but anonymous disclosures will run counter to the transparency and the accountability that the PDA attempts to promote and should not be encouraged. Employees should be warned that anonymous disclosures might impede an investigation.[52] Despite this, it is nevertheless suggested that procedures should be available to accommodate and investigate anonymous disclosures. Employees may not have confidence in the reporting system: the information could still be true and, if ignored, may encourage a general disclosure that could embarrass the employer. It is important that employees be assured that no action will follow if *bona fide* concerns turn out to be groundless, but that malicious allegations may result in disciplinary action.

---

[51] Bowers, Lewis and Mitchell op cit (n5) at 146-8.

[52] L Camerer 'The Protected Disclosures Act, No 26 of 2000' (2001) *ISS Paper* 47.

Both regulators/confidants and employees should be trained. In particular, the type of issues and the manner of feedback should be known to all concerned. Regarding corruption, the employer should provide very clear guidelines on the receipt and size of gifts and entertainment and on the meaning of corruption. In a society imbued with corrupt conduct, not all may be clear on its exact meaning.

While not specifically designed to fight corruption and despite its shortcomings, the PDA, particularly s 6, can be a useful early warning system since it enables the employer to tap into one of its best resources: its employees.

(b) Entrapment

Section 252A(1) of the Criminal Procedure Act 51 of 1977 ('the CPA') permits entrapment and undercover operations to detect or investigate criminal acts, provided these do not go beyond providing an opportunity to commit an offence. When the entrapment goes beyond providing an opportunity to commit an offence, evidence so obtained may still be admissible. However, in terms of s 252A(3), the court will be required to weigh up the public interest against the personal interest of the accused. This provision remains subject to the provisions of s 35(5) of the Constitution, which excludes unconstitutionally obtained evidence if it would render the trial unfair or otherwise be detrimental to the administration of justice. (It is, however, to be noted that s 35(5) is not applicable to civil proceedings.[53])

The CPA, however, does not have direct application in the workplace. In *Cape Town City Council v SAMWU & others*[54] the court was required to consider the use of traps at the workplace. Stelzner AJ indicated that, provided that the entrapment is properly scrutinized and the admissibility of the evidence regulated, there may well be circumstances in which evidence obtained by means of a trap should be used[55] and suggested that s 252A of the CPA be used as a guideline in the employment context.[56] *In casu* the evidence was rejected on the basis, *inter alia*, that the employees concerned were not under suspicion at the time of the trap; that they had not agreed to the proposal made to them on the first approach and that those who set the trap enriched themselves by failing to hand over to the employer all the proceeds resulting from the trap.[57] In subsequent arbitration awards, commissioners have tended to accept evidence procured by means of a

[53] See PJ Schwikkard and SE van der Merwe *Principles of Evidence* 2ed (2002) 248-9.
[54] (2000) 21 *ILJ* 2409 (LC).
[55] 2434F.
[56] 2435A.
[57] 2435E-2436B.

trap, provided that the trap in question did not amount to a temptation. Evidence resulting from a trap has also been accepted where such trap was randomly set but preceded by a warning of random traps.[58] In *SATAWU obo Assegai v Autopax*[59] the arbitrator was prepared to accept video evidence about a transaction made during the course of the employee's duty, even though the employee was unaware of the recording.[60]

There may well be circumstances where such recording amounts to an invasion of privacy, in which case a balancing of interests, as discussed below with reference to telephone tapping and e-mail interception, should be conducted: Although section 35(5) of the Constitution is not applicable to civil proceedings, an employee still has a right to a fair civil trial in terms of s 34 of the Constitution.[61]

(c) Gifts

The line between a gift and a bribe is sometimes extremely thin. Clear guidelines on the limits of gifts, while not a legal tool, will certainly assist in making this distinction. Some have suggested (in the context of grand corruption) that a reasonable maximum level for small gifts would be 2% of the gross contract value or $20 000, 00, whichever is the lesser.[62]

It is doubtful whether such a limit is wise. The Prevention of Corruption Bill 2002 does not place a monetary limit on the value of gratification and a gift of any value could therefore attract the consequences of the Bill. It is suggested that the court will in all instances consider the purpose of the gratification rather than its value. What is more, in many instances, a gift of this nature (2% of the gross contract value or $20 000, 00) will be sufficient to induce corruption and to compromise decision-making.

Having said that, it is not suggested that there is no room for hospitality and gratitude, but it is paramount that employers have clear policies (and perhaps even a 'clearing system') on the reporting of the offer and acceptance of gifts and hospitality. Employers should not hesitate to instruct an employee not to accept or to return a gift that is considered inappropriate.

---

[58] See *SATAWU obo Radebe v Metrorail Wits* [2001] 9 BALR 976 (AMSSA) and *SATAWU obo Sefara v Metrorail Services, Pre*toria [2001] 9 BALR 976 (AMSSA).

[59] [2002] 2 BALR 171 (AMSSA).

[60] This is consistent with the judgement in *Pretoria Technology Limited v Wainer* [1997] 3 *All SA* 594 (W) at 609d.

[61] Schwikkard and Van der Merwe op cit (n53).

[62] Moody-Stuart op cit (n16) at 59.

Workplace privacy

Corrupt activities by definition do not happen overtly and are often discovered by accident. Employers may accordingly need to monitor the less public aspects of their employees' activities, such as their communications. This brings another aspect of South African law into the fight against corruption, namely, the right to privacy.[63]

Section 14(d) of the Constitution provides that everyone has the right to privacy, which includes the right not to have the privacy of his or her communications infringed. However, privacy is not an absolute right and will always involve the balancing of competing rights such as the common law right of the employer to preserve its property and society's interest in eradicating unlawful conduct.[64]

In foreign jurisdictions, particularly the USA, an employee's right to privacy at the workplace is fairly limited.[65] Even in South Africa, the scope of the right to privacy in general, and more specifically the right to privacy at the workplace, remains vague. In *Bernstein and Others v Bester NO and Others*,[66] Ackerman J emphasized that, while privacy is acknowledged in respect of a person's inner sanctum (such as family life, sexual preference and home environment), protection erodes as he or she moves into communal relations and activities such as business and social interaction. It was with this judgement as authority that the court in *Wainer* held that an employee's privacy was not violated when his employer taped telephonic conversations of the employee relating to the employer's affairs.[67] Heher J indicated[68] that should he be wrong in this conclusion, the invasion of privacy would nevertheless be justified in terms of section 36 of the Constitution (this aspect will be reverted to below).

Unfortunately, arbitration awards by CCMA commissioners dealing with privacy in the workplace have not provided any clear guidelines. The

---

[63] Apart from corruption there are compelling reasons for employer surveillance of employee's electronic communications. These include performance monitoring, employee productivity, avoidance of criminal and civil liability and protection of security of computer systems. See M Paterson 'Monitoring of employee emails and other electronic communications' (2002) 21 *University of Tasmania Law Review* 1 at 2-8 and M Jeffery 'Information technology and worker's privacy: Introduction' (2002) 23 *Comparative Labor Law & Policy Journal* 251 at 268-73.

[64] *Protea Technology Limited v Wainer* op cit (n60) at 611f-g.

[65] D Collier 'Workplace privacy in the cyber age' (2002) 23 *ILJ* 1743 at 1755-8. Also see Jeffery op cit (n63) at 277-8.

[66] 1996 (4) BCLR 449 (CC) at 792G-I, 793E and 795D.

[67] Op cit (n60) at 608f-610e.

[68] At 610f.

commissioner in *Moonsamy v The Mailhouse*[69], unlike the judge in *Wainer*, was not prepared to accept that the recording of an employee's telephone calls in his office was not an invasion of the employee's constitutional right to privacy and proceeded to test whether the invasion could be justified in terms of section 36 of the 1996 Constitution, ultimately finding in favour of the employee. In *Sugreen and Standard Bank of SA*,[70] commissioner Rycroft indicated that the use of telephones and e-mail facilities provided by the employer are 'legitimate areas of interest to the employer where it suspects that the employee is guilty of misconduct'[71].

Cyber privacy and legislation

The question is whether recent legislation such as the Electronic Communications and Transactions Act 25 of 2002[72] ('the ECT') and the Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002[73] ('the RICA') have provided any clearer guidelines.

One of the most significant provisions of ECT is s 86(1)[74], which provides that it is a crime for an employer to access or intercept not only e-mail messages and telephone conversations, but all other data stored on an employee's computer without *authority* or *permission* to do so.

The scope of RICA is narrower in that it only regulates communications as opposed to (electronic) data in general. Section 2 of RICA provides that no person may intentionally intercept[75] any communication in the course of its occurrence or transmission. This appears to block the way for any form of workplace monitoring, but a number of exceptions are provided for in RICA. The exceptions in ss 5 and 6 are particularly relevant to the workplace.

Section 5(1) provides that any person may intercept any communication if one of the parties to the communication has given prior consent in writing to

[69] (1999) 20 *ILJ* 464 (CCMA).
[70] (2002) 23 *ILJ* 1319 (CCMA).
[71] At 1323F-G.
[72] The Act came into operation on 30 August 2002.
[73] The Act was assented to on 30 December 2002, but the date of commencement is yet to be proclaimed.
[74] This provision is subject to the Interception and Monitoring Prohibition Act 127 of 1992. This Act prohibits interception and monitoring of communications except if so ordered by a judge on application of the police, defence force, national intelligence agency or the directorate of Special Operations as defined in the National Prosecuting Authority Act 32 of 1998. It does not make provision for an employer to make such an application. The Act (to be repealed once RICA comes into force) accordingly has limited relevance to the employment relationship and is therefore ignored for the purpose of this note.
[75] This is defined to include monitor, view, examine or inspect. See s 1.

such interception.[76] It is suggested that the most appropriate method of securing such consent is by obtaining it in the contract of employment.

Where such consent does not exist or cannot be obtained, the employer may still be able to rely on the provisions of s 6(1), which provides that any person may, in the course of carrying on any business, intercept any *indirect communication* that, *inter alia*, relates to that business or which otherwise takes place in the course of the carrying on of that business.[77] RICA defines indirect communications as the transmission of information including data or text by means of a postal service or a telecommunication system.[78] Since an employee is supposed to advance the interests of his or her employer during normal hours of work, the reference to communication 'that takes place in the course of the carrying on of that business' is probably wide enough to include all communications that occur while the employee is at the place of work. That, however, is not the end of the inquiry. The interception will only be acceptable if a number of requirements are met. These requirements are listed in s 6(2) and include:

1. The consent of the system controller which, in the case of a juristic body, includes, amongst others, the chief executive officer or equivalent officer of the juristic person or any person duly authorized by that officer;
2. The interception must be for the purpose of monitoring or record-keeping of indirect communications in order to establish facts (in other words to obtain evidence); to detect unauthorized use of the telecommunication system or to secure the effective operation of the system;
3. The telecommunication system must be provided in connection with that business; and
4. The system controller must make reasonable efforts to inform the person using the system that indirect communications may be intercepted, or alternatively, the consent of the employee must be obtained either expressly or impliedly.

---

[76] For a discussion of the meaning of consent in comparative law see RB Filho and M Jeffery 'Information technology and worker's privacy: Notice and consent' (2002) 23 *Comparative Labor Law & Policy Journal* 551 at 552-60.

[77] 'Business' is defined in s 1 to mean any business activity conducted by any person, including activities of any private or public body, but it is not clear to what extent the Act will apply if the place of work is not a business in the conventional sense, but a charity organization, church or NGO. It is suggested that the application of the Act will be severely limited if business is interpreted too narrowly.

[78] Section 1.

The provisions of s 6 clearly provide scope for the employer to intercept indirect communications via systems provided by the employer such as e-mail and telephones, provided that there is notification[79] in advance or consent.[80] RICA does not require that notice be given immediately prior to the interception. It can therefore be in a notice circulated by the employer from time to time. A further safeguard that the employer can utilise is to inform the employees – again either in the contract or by general notice – as to what type of use will be regarded as unauthorized. The Employment Practices Data Protection Code 2003, issued in terms of the UK Data Protection Act 1998[81], provides some useful guidelines in this regard. The Code emphasizes the need to set out clearly the restrictions on the use of systems (including Internet) provided by the employer and the extent to which these systems may be used for private purposes, if at all. The Code also encourages employers to provide alternatives for private communications, e.g. an internal post for communications with the company doctor or the human resources department.

RICA, in the context of corruption, has its limitations. Unless the consent contemplated in s 5 is obtained, s 6 does not cover a situation, such as arose in *Wainer*, where a recording device was placed in the employee's office to record cellular calls on a private phone, and it does not regulate access to data, other than e-mail communications, stored on the employee's computer. In such cases, the ECT will regulate the situation.[82]

While it is true that a court still has discretion to admit illegally obtained evidence in a civil dispute[83], an employer can minimise the risk of criminal

---

[79] For a discussion of the meaning of notice in comparative law see Filho and Jeffery op cit (n76) at 560-6.

[80] The question is whether such notification as contemplated in s 6 of RICA, when not dealt with in the contract of employment, will amount to a unilateral change in the conditions of employment that may warrant strike action in terms of s 64(4) of the LRA. Apart from the fact that RICA requires no more than notification, it is doubtful whether our courts will regard such notification as a unilateral change of the conditions of employment. Unless the notification changes the work that the employee originally agreed to perform under the terms of his or her contract *NUMSA v Escom* [2001] 10 BLLR 1144 (LC), or amounts to such great variation of the work contemplated in the contract of employment that it results in a 'major work reorganisation' *NUMSA v Lumex Clipsal (Pty) Ltd* [2001] 2 BLLR 220 (LC), it is submitted that such a notice sits comfortably within the realm of managerial prerogative.

[81] For a discussion of this act see M Jeffery 'Information and worker's privacy: The English law' (2002) 23 *Comparative Labor Law & Policy Journal* 301.

[82] Section 86(1).

[83] See *Protea Technology Limited v Wainer* op cit (n60) at 606f and *Tap Wine Trading CC v Cape Classic Wines (Western Cape) CC* 1999 (4) SA 194 (C) at 198H. Also see *S v Kidson* 1999 (1) SACR 338 (W).

liability[84] by obtaining the authority or permission contemplated in s 86(1) of ECT.

It is suggested that authority or permission in this context (ECT) relates to consent by the employee or authority obtained from a court of law.

In *Moonsamy*[85], the commissioner, with reference to s 158 of the LRA, held that the Labour Court should have the power to authorize telephone tapping provided that sufficient evidence is placed before the court indicating that the employer is suffering loss as a result of the employee's conduct and that there is no alternative method to obtain evidence. Since it would hardly be ideal to alert a potential transgressor by approaching him or her for permission or by initiating a court application, it is suggested that the contract of employment remains the ideal vehicle to secure such consent. Such consent will minimise the risk of criminal liability in terms of both ECT and RICA. Regarding consent obtained via the contract of employment, the commissioner in *Moonsamy* warned[86] that this will not be sufficient unless it can be shown that the employee at the time of concluding the contract had a proper appreciation of the nature and the extent of the act being consented to.

Section 36(1) of the Constitution

Where prior consent was obtained or the required notification occurred, criminal liability may be avoided but employers should still be conservative in relying on such consent/notification. As stated above, the employment relationship is essentially a relationship of trust. The notion of a "big brother" employer perpetually spying on the activities of employees may put this relationship, along with staff morale, in serious jeopardy. In instances where evidence was obtained (illegally) by invading the individual's privacy, the courts and CCMA have balanced the employer's right to economic activity with the employee's right to privacy in accordance with the limitation clause – s 36 of the Constitution.[87] It is suggested that, whether or not consent/notification measures are in place, employers should always taper the need to invade an employee's privacy with reference to s 36(1) of the Constitution:

'The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including–

---

[84] Any interception falling foul of the provisions of RICA and ECT will constitute an offence and hefty fines (up to R2 000 000, 00 in the case of RICA) or imprisonment may be imposed. See s 51 of RICA and s 89(1) of ECT.

[85] Op cit note 69 at 473E-F.

[86] At 474A.

[87] *Protea Technology Limited v Wainer* op cit (n60) at 611a-c and *Moonsamy v The Mailhouse* op cit (n69) at 469E.

(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.'

It is generally accepted that 'a law of general application' includes the common law.[88] In this instance it is the common law right of the employer to protect its property and business interests that may potentially limit the employee's right to privacy. The weight of factors listed in s 36(1) can only be determined with reference to the facts of the particular case, but it is suggested that the following principles will guide a presiding officer called upon to decide the matter:

1. The extent to which the employee harbours a subjective expectation of privacy that society will regard as objectively reasonable. This will be determined by the operational realities of the workplace, but also the efforts of the employer to alert employees by means of notification or informed consent of such possible invasions, as well as clear policies on private activities at the place of work. In the latter regard employers should guard against creating a false expectation of privacy by not reminding employees of the terms of a contract or by failing to repeat or execute notifications of monitoring.
2. The right to privacy is specifically protected in the Constitution. However, while the right to economic activity was protected in the interim Constitution, no similar protection was included under the final Constitution. This, according to Commissioner Van Dokkum in *Moonsamy*[89], signals a clear intention that the 'employee's personal rights are preferred to the more amorphous (and consequently controversial) right to economic activity'. This, it is submitted, means no more than that clear evidence must exist that the employer's business is seriously threatened.[90]

[88] J De Waal, I Currie and G Erasmus *The Bill of Rights Handbook* 4ed (2001) 148.
[89] Op cit (n69) at 471G-H.
[90] In this regard, patterns in empirical data present an interesting question. Auditors may, through data mining, discover some odd patterns in financial statements. Such patterns do not prove anything, but may be an indication that mischief is afoot. Can such patterns form the basis for monitoring telephone calls or e-mails more closely? It is suggested that the answer to this should be yes, but only because these patterns combined with other factors, strongly pointed to irregular conduct. Odd patterns alone, it is suggested, should be treated with great circumspection.

3. The extent to which similar evidence can be secured by conventional means or, in the absence of such means, the extent to which prior notification was made or whether consent was obtained from the employee or, alternatively, authorization was obtained from a court. If reliance is placed on prior consent (e.g. obtained in the contract of employment), it must be supported with evidence that the employee had a clear understanding of what was consented to.

It is suggested that the following summary of comparative law is also true of the South African position:

> 'Thus, in all cases – whether we are dealing with surveillance or data processing (or, indeed, whether the law takes them to be the same thing); whether the question of privacy arises in a case on the propriety of disciplinary action or dismissal, on a question of contractual good faith, on the application of data processing laws, or any other matter; whether or not there has been notice and consent; and, whether the legal system establishes the irreducible minimum of privacy protection at a higher or lower level – the matter usually boils down to a question of what is or is not reasonable for employers to do in the particular circumstances of the particular case.'[91]

Conclusion

While prevention remains better than cure, much of what has been said above relates to the gathering of evidence after the fact. Regarding prevention, it is suggested that the employer can do no more than remind employees of their duty to act in good faith. This can be done by constant reminders of what the employer is entitled to do in respect of the gathering of evidence and promoting reliable channels for *bona fide* whistleblowers. The truth, however, is that employers are powerless to address corrupt minds. For that they cannot be held accountable. Rather, it is in terms of how employers manage corruption, an issue that largely revolves around the crafting of contracts of employment and the gathering of evidence, that they (and, ultimately, perceptions of corruption) will be judged.

Admittedly, very limited legislative means are available to employees to address corruption in the workplace, but this does not imply that they should be passive bystanders: after all they remain a very important source of information. Of those discussed above, only whistleblowing provides legislative means to employees to address corruption in the workplace and it is paramount that the best be made of this, despite its shortcomings. In this regard, trade unions can play an important role in not only facilitating the

[91] Jeffery op cit (n63) at 276.

introduction of whistlebowing procedures in the workplace, but also by encouraging employees to use these procedures.

Although there will always be scope for more effective deterrents, there are aspects of South African law that provide a framework within which employers (and, to a limited extent, employees) can establish a useful anti-corruption strategy. It will, however, require a commitment from both employers and employees to engage with these laws.