LEGALITY OF MONITORING E-MAIL AT THE WORKPLACE:

A LEGAL UPDATE

Ms Heidi Schoeman (Advocate of the High Court of South Africa) and Ms Mariëtte Jones

(Attorney of the High Court of South Africa)

Technikon Witwatersrand Technikon Witwatersrand

heidscho@mail.twr.ac.za; mwjones@mail.twr.ac.za

Tel: 011 – 406 3588

P O Box 17011, Doornfontein, 2028

ABSTRACT

It seems fair to assume that employers provide e-mail facilities to employees as tools intended for work-related activity. As such it further seems fair to assume that employers would have the right to monitor such e-mail messages. However, the question arises as to how far the right to privacy – one of the fundamental rights contained in the Bill of Rights in the South African Constitution – may curtail an employer's assumed right to the monitoring of an employee's e-mail communications.

Section 14 of the Constitution states that everyone has the right to privacy, which shall include the right not to have their person or home searched; their property searched; their possessions seized; or *the privacy of their communications infringed.* It is said that section 14 protects information to the extent that it limits the ability to gain, publish, disclose or use information about others.

While stressing the importance of the right to privacy, the Constitutional Court nevertheless stated that "the protection accorded to the right of privacy is broad but it can also be limited in appropriate circumstances", and that the scope of a person's privacy should extend only to those areas where he/she would have a *legitimate expectation* of privacy.

In December 2002, the President assented to the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA). RICA prohibits the interception of communication (inclusive of direct and indirect communication), unless it is intercepted by a party to the communication, or if an author of the communication has consented thereto. Law enforcement officers may intercept communications under certain conditions.

In the case of the interception of indirect communications in the business environment, same may only be intercepted in accordance with the provisions of section 6 of RICA. This means, amongst others, if the person who is a party to the communication is aware of the fact that the communications could be intercepted.

Employers had previously successfully intercepted e-mail communications of employees, which had resulted in some highly publicised dismissals. RICA is now placing an obligation on the organisation, which usually means the IT Department, to inform employees of the organisation's intention to intercept both direct and indirect communications.

The aim of this paper is to provide the legislative framework within which organisations may intercept e-mail communications of its employees.

KEY WORDS

Right to privacy – limitation of fundamental rights – interception – work place - dismissal

LEGALITY OF MONITORING E-MAIL AT THE WORKPLACE:

A LEGAL UPDATE

1. EXECUTIVE SUMMARY

It seems fair to assume that employers provide e-mail facilities to employees as tools intended for work-related activity. As such it further seems fair to assume that employers would have the right to monitor such e-mail messages. However, the question arises as to how far the right to privacy – one of the fundamental rights contained in the Bill of Rights in the South African Constitution[1] – may curtail an employer's assumed right to the monitoring of an employee's e-mail communications.

Section 14 of the Constitution states that everyone has the right to privacy. While stressing the importance of the right to privacy, the Constitutional Court nevertheless stated that "the protection accorded to the right of privacy is broad but it can also be limited in appropriate circumstances"[2], and that the scope of a person's privacy should extend only to those areas where he/she would have a *legitimate expectation* of privacy[3].

In December 2002, the President assented to the Regulation of Interception of Communications and Provision of Communication Related Information Act[4]. RICA prohibits the interception of communication (inclusive of direct and indirect communication), unless it is intercepted by a party to the communication, or if an author of the communication has consented thereto. Law enforcement officers may intercept communications under certain conditions.

In the case of the interception of indirect communications in the business environment, same may only be intercepted in accordance with the provisions of section 6 of RICA. This means, amongst others, if the person who is a party to the communication is aware of the fact that the communications could be intercepted.

Employers had previously successfully intercepted e-mail communications of employees, which had resulted in some highly publicised dismissals. RICA is now placing an obligation on the organisation, which usually means the IT Department, to inform employees of the organisation's intention to intercept both direct and indirect communications.

The aim of this paper is to provide a brief Constitutional analysis of the South African legislative framework within which organisations may intercept e-mail communications of its employees.

2. INTRODUCTION

The right to privacy is one of the fundamental rights contained in the Bill of Rights in the South African Constitution. Our Courts have interpreted the application of section 14 as an important but not an absolute fundamental right. In certain instances this right may be limited in accordance with section 36. A brief overview of selected case law will be provided in this regard.

The second part of this discussion will focus on the right to privacy in the work place vs. the employer's right to have its information systems not abused by employees. Particular attention will be paid to section 6 of RICA to which the President assented on 30 December 2002.

---

[1] Act 108 of 1996, herein referred to as the Constitution.
[2] Madala J in *Case and Another v Minister of Safety and Security* 1996 3 SA 617 (CC) at 661E.
[3] *Bernstein and Others v Bester and Others NNO* 1996 2 SA 751 (CC).
[4] Act 70 of 2002, herein referred to as RICA.

3. RIGHT TO PRIVACY

3.1 INTRODUCTION

Section 14 of the Constitution states that everyone has the right to privacy, which shall include the right not to have their person or home searched; their property searched; their possessions seized; or *the privacy of their communications infringed*[5]. It is said that section 14 protects information to the extent that it limits the ability to gain, publish, disclose or use information about others[6].

3.2 RIGHT TO PRIVACY THROUGH THE CASES

That a high premium was to be placed on the right to privacy in the new South Africa became clear soon after the Interim Constitution [7] was adopted. Ackerman J analysed and discussed the concept of personal privacy in the Constitutional Court case of *Bernstein v Bester*[8], and stated that a very high level of protection should be given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions, and that there was a final untouchable sphere of human freedom that was beyond any interference from any public authority.

In a subsequent case[9], Langa DP elaborated on the above by clearly stating that the right to privacy does not relate solely to the individual within his or her intimate sphere:

> "[W]hen people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the State unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play."

In *Case v Minister of Safety and Security*[10] the accused successfully challenged the constitutionality of statutory charges relating to the possession of pornography[11].

It is important to note, however, that like most other fundamental rights, the right to privacy is not absolute. While stressing the importance of the right to privacy, the Constitutional Court in the *Case* matter also stated that "the protection accorded to the right of privacy is broad but it can also be limited in appropriate circumstances"[12], and that the scope of a person's privacy should extend only to those areas where he/she would have a *legitimate expectation* of privacy[13].

---

[5] Section 14(d).
[6] McQuoid-Mason *Constitutional Law of South Africa* "Privacy" 1998 18.
[7] The Constitution of the Republic of South Africa Act 200 of 1993 herein referred to as "the Interim Constitution".
[8] *Bernstein op.cit.*
[9] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 1 SA 545 (CC).
[10] *Case and Another v Minister of Safety and Security and Others* 1996 3 SA 617 (CC); *Curtis v Minister of Safety and Security and Others* 1996 3 SA 617 (CC).
[11] Viz. the prohibition on the possession of indecent or obscene photographic matter in terms of s 2(1) of the *Indecent or Obscene Photographic Matter Act* 37 of 1967. In para 91 of *Case* (op.cit.) Didcott J held "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 certainly is 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 section 13 of the Interim Constitution…guarantees that I shall enjoy."
[12] Madala J in *Case op.cit.* para 106.
[13] *Bernstein op. cit* para 75.

It has been pointed out that a "legitimate expectation of privacy" will be that which society recognises as an objectively reasonable expectation of privacy[14]. This in turn means that a person cannot complain about an invasion of privacy if he/she has consented to having his/her privacy invaded, which consent may be express or implied.

In the *Bernstein* case supra, Ackerman J in his analysis of the *continuum* on which the legitimacy of an expectation of having one's privacy respected may fall, noted that "[t]his inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation."[15]

From the most recent Constitutional Court case dealing with, *inter alia* the right to privacy, it furthermore becomes clear that a person's expectation of having his/her privacy respected does not extend to unlawful activities committed in private. In *S v Jordan and Others (Sex Workers Education and Advocacy Task Force and Others as Amici Curiae)*[16], certain statutory provisions criminalizing prostitution and the keeping of brothels[17] were challenged as being unconstitutional on several grounds[18] including the right to privacy. Having established that the offences of prostitution and brothel-keeping are *not* unconstitutional, Ngcobo J said that[19]

> "I do not accept that a person who commits a crime in private, the nature of which can only be committed in private, can necessarily claim the protection of the privacy clause…The law should be as concerned with crimes that are committed in private as it is with crimes that are committed in public."

3.3 LIMITATIONS

Apart from the general limitations placed upon the right to privacy discussed above, Section 36 of the Constitution, the so-called "limitations clause", specifically allows a limitation of a fundamental right in certain circumstances. The section reads as follows:

> "(1) 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 –
>
> (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.

---

[14] De Waal *et al The Bill of Rights Handbook* 1998 212.
[15] *Bernstein* (op.cit.) para 77.
[16] 2002 6 SA 642 (CC).
[17] Sections 2 and 3(b) and (c) of the *Sexual Offences Act* 23 of 1957 outlawed the keeping of a brothel, while section 20(1)(aA) of the same Act made it an offence to have unlawful carnal intercourse or commit an act of indecency for reward.
[18] These grounds included, inter alia, unfair discrimination based on gender, as the Act criminalized only the activities of the prostitute and not those of the client. In the judgement by Ngcobo J it was pointed out in para 14 that both at common law and in terms of the *Riotous Assemblies Act* 17 of 1956 the customer [of a prostitute] commits an offence and in terms of the *Riotous Assemblies Act* the customer is liable to the same punishment to which the prostitute is liable.
[19] *S v* Jordan (op.cit) para 28.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights."

From the above it is clear that a right can only be limited if the limitation is authorised by "a law" and the law itself must be of general application. The right is then limited, but only insofar as it is justifiable in a democratic society. Whether or not it is justifiable depends on the criteria set out in subsections 36(1)(a)-(e).

3.4 SECTION 36 THROUGH THE CASES

In considering the constitutionality of the death penalty, the Constitutional Court in S *v Makwanyane*[20] formulated certain guidelines concerning the application of the general limitations clause in the interim Constitution[21]. It was pointed out that the limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society is ultimately an assessment based on proportionality. This in turn calls for the weighing up of the purposes, effects and importance of the infringing legislation against the nature and effect of the infringement caused by the legislation. The more severe the limitation/s of a fundamental right, the more compelling the reasons for its justification should be[22].

In *Makwanyane* the court weighed up the rights to life, to human dignity and to freedom from inhuman or degrading punishment against the purposes of the death penalty, viz. as a deterrent to violent crime and its recurrence and as a fitting retribution for such crimes[23]. The court found that, given the drastic effects of the death penalty, a far less restrictive means of achieving the same purpose, namely life imprisonment, should be preferred[24].

The balancing approach formulated in *Makwanyane* was subsequently applied in several cases. In *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*[25] the Constitutional Court was asked to adjudicate upon the constitutionality of various statutory prohibitions concerning sodomy[26]. After finding that the criminalisation of sodomy infringed the right to privacy in section 14 of the Constitution[27], the Court enquired whether such infringement of the right to privacy could be justified in terms of s 36 of the Constitution. It was held that such limitation was unjustifiable as it was a *severe* limitation of the right[28], the limitation itself served no valid purpose[29], and furthermore, an analysis of the jurisprudence of other open and democratic societies based on human dignity, equality and freedom on balance supported the conclusion that sodomy was unjustifiable[30].

---

[20] 1995 3 SA 391 (CC).
[21] *S v Makwanyane* (op.cit.) para 104.
[22] See *S v Bhulwana* 1996 1 SA 388 (CC) para 18. See also *S v Manamela and Another (Director-General of Justice intervening)* 2000 3 SA 1 (CC) para 32.
[23] *S v Makwanyane* (op.cit.) para 117 and para 185.
[24] *S v Makwanyane* (op.cit.) para 128. See also para 184 in which Didcott J questions the deterrent effect of the death penalty.
[25] 1999 1 SA 6 (CC).
[26] Viz. section 20A of the *Sexual Offences Act* 23 of 1957; the inclusion of sodomy as an item in Schedule 1 to the *Criminal Procedure Act* 51 of 1977 and the inclusion of sodomy as an item in the Schedule to the *Security Officers Act* 92 of 1987.
[27] *National Coalition for Gay and Lesbian Equality* (op.cit.) para 32.
[28] *Ibid* para 36.
[29] *Ibid* para 37.
[30] *Ibid* para 39 read with para 57.

In *S v Manamela* the reverse onus provision of the *General Law Amendment Act*[31] was weighed up against the right of arrested, detained and accused persons to remain silent[32]. It was held that the effective prosecution of crime was a societal objective of great significance which could, where appropriate, justify the infringement of fundamental rights[33], and that it outweighed the right to silence in this instance[34].

Ultimately therefore, the purpose of any given law will be weighed up against the importance of the fundamental right that it stands to infringe.

3.5 RIGHT TO PRIVACY IN THE WORK PLACE

The Constitutional Court has not yet been called upon to make a ruling regarding the application of section 14 in the work place. Some of our other Courts have, however, had to address this aspect. A brief overview of cases dealing with the interception of telephone conversations and e-mails at the work place is provided below.

3.5.1 INTERCEPTION OF TELEPHONE CONVERSATIONS

The *Moonsamy v The Mailhouse* case[35] sets the South African precedent for an employee's right to privacy at the workplace. In this case an employee was dismissed as a result of the tape recording of his telephone conversations at work having been made by the employer without his consent. After his dismissal, the employee referred the matter to the CCMA[36]. He alleged that the tape recordings were obtained in contravention of the Interception and Monitoring Prohibition Act[37]. The Commissioner rejected the argument that the IMPA was applicable to individuals. Moreover, it was held the IPMA did not render all evidence obtained contrary to the provisions thereof inadmissible.

The employee further contended that his right to privacy, as guaranteed in the Constitution, was breached through the actions of the employer. As both parties had agreed that the Constitution is applicable to the dispute, it was held that the interception of the employee's telephone conversations was indeed in breach of section 14 of the Constitution. The Commissioner had to, however, decide whether this infringement could be justified by the limitations clause. It was held that telephone conversations by their nature are very private. As such, they may not be infringed upon without prior authorisation: Provided that the employer shows compelling business necessity reasons for the disclosure of such conversations. On the facts it held that the employer had other means to its disposal to obtain evidence against the employee. As such, it was found that the interception of the telephone conversation without prior authorisation was *contra* the Constitution and therefore inadmissible.

In *Protea Tech v Weiner*[38] the Court also had to decide whether or not the interception of telephone conversations by an employer of an employee was admissible. The facts in this case

---

[31] Act 62 of 1955, section 5. This section provided for an accused to prove that she or he had reasonable cause for believing that goods acquired or received were the property of the person from whom they were received or that such person had the authority of the owner to dispose of them.
[32] S 35(1)(a) of the Constitution.
[33] *S v Manamela* (op.cit.) para 27.
[34] *Ibid* para 38 where it was held that "there was nothing unreasonable, oppressive or unduly intrusive in asking an accused who had already been shown to be in possession of stolen goods, acquired otherwise than at a public sale, to produce the requisite evidence, namely that she or he had reasonable cause for believing that the goods were acquired from the owner or from some other person who had the authority of the owner to dispose of them."
[35] 1999 20 ILJ 464 (CCMA). Please note that the award is only binding on the parties to the dispute.
[36] Commission for Conciliation, Mediation and Arbitration.
[37] Act 127 of 1992, herein referred to as IMPA. The IMPA was repealed by section 62(1) RICA.
[38] 1997 9 BCLR 1225 (W).

differ from the *Moonsamy* case in that the primary consideration in this case was that of unlawful competition as opposed to that of an unfair dismissal. Insofar as the question relates to the breach of the right to privacy by the employer, the Court held that where a an employer / employee relationship exists and where telephone conversation takes place during business hours from the employer's premises, the conversations were not private and as such they are not protected by the Constitution. Moreover, a Court has a discretion to allow (or disallow) evidence that was obtained illegally, depending on the facts of each case, and in accordance with the provisions of section 36(1) of the Constitution.

Waste Products Utilisation (Pty) Ltd v Wilkes[39] confirmed that a Court has a discretion to determine whether or not to admit tape recordings that were obtained in an improper manner or in the infringement of a constitutional right. The application of the Constitution is pre-emptive but the rights set out in the bill of rights are not absolute.

3.5.2 INTERCEPTION OF E-MAIL

As yet, there are no reported court cases dealing directly with the intercepting and monitoring of e-mails at the workplace. Two instances of such monitoring deserve mention, however.

In and during 1990 Toyota dismissed an employee who e-mailed messages of the Zimbabwean President superimposed on a gorilla. The CCMA found that the e-mail messages, as well as the hard copies that were distributed, were racist in nature. The CCMA also upheld dismissal as an appropriate sanction[40]. Unfortunately this case was not reported and therefore the reasoning informing the finding is not available.

The so-called Energiser Holdings case has received much media attention. A number of employees were charged with, and found guilty of, having contravened the company's e-mail policy by having received and sent various pornographic, racist and other personal e-mails. These e-mails were intercepted without the employees' knowledge. The employees alleged that the company had no clear policy regarding the utilisation of its e-mail facility[41]. The matter was referred to private arbitration and the findings are therefore not a matter of public record. From an academic point of view this is unfortunate as a legal pronouncement on this issue would have been invaluable.

In sum, therefore - at present there are no reported cases dealing directly with the interception and monitoring of e-mails at the workplace, and only a handful of cases dealing with the monitoring of phone calls at the workplace. Furthermore, it is difficult to try and predict the courts' reasoning by using the latter cases as an analogy, as they resulted in conflicting findings. Against this background the relevant provisions of a newly enacted Statute dealing specifically with this issue, viz. the Regulation of Interception of Communications and Provision of Communication Related Information Act[42] will now be examined.

4. REGULATION OF THE INTERCEPTION OF COMMUNICATIONS ACT (RICA)

4.1 INTRODUCTION

---

[39] 2003 2 SA (W) 550F. Please note that this case dealt with a delictual claim based on unlawful competition by an employee with his employer. On the facts it was found that the tapes that were secured illegally, but the other party had tried to deceive the Court. As such, the tapes were admitted into evidence.

[40] Sukhraj P "New law stops bosses spying on e-mail" *Sunday Times* 2 February 2002 5.

[41] *Ibid*.

[42] *Op.cit.*.

Both the Toyota and the Energiser Holdings-cases occurred prior to the entry into force of RICA in 2003. RICA brings about legislative certainty regarding the prohibition of the interception[43] of direct[44] and indirect[45] communication albeit that the interpretation of RICA is still in the hands of our Courts. There are, however, exceptions to the rule. For example[46], communications may be intercepted by a party to the communication[47], if an author of the communication has consented thereto[48], or by law enforcement officers under certain conditions[49].

4.2 APPLICATION OF RICA

Section 6[50] of RICA specifically regulates the interception of indirect communications at the work place. The question begs what are the implications of section 6 for the employer?

---

[43] Section 1 defines intercept as meaning "aural or other acquisition of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the –

(a) monitoring of any such communication by means of a monitoring device;
(b) viewing, examination or inspection of the contents of any indirect communication; and
(c) diversion of any indirect communication from its intended destination to any other destination,

and "interception" has a corresponding meaning."

[44] Defined in section 1 as meaning "an –

(a) oral communication, other than an indirect communication between two or more persons which occurs in the immediate presence or all the persons participating in that communication; or
(b) utterance by a person who is participating in an indirect communication if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication".

[45] Defined in section 1 as meaning "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 animated or not; (v) signals; or (vi) radio frequency spectrum; or
(b) in any other form or in any combination of forms".

[46] It is also permissible to intercept communications in order to prevent serious bodily harm (section 7); in the case of certain emergencies in order to determine location (section 8) or if another act authorises the interception of the communication (section 9), for example in terms of the Correctional Services Act 111 of 1998.

[47] RICA section 4.

[48] RICA section 5.

[49] RICA section 4(2), read together with section 16(1)(a).

[50] "(1) Any person may, in the course of the carrying on of any business, intercept any indirect communication –

(a) by means of which a transaction is entered into on behalf of that business;
(b) which otherwise relates to that business; or
(c) which otherwise takes place in the course of the carrying on of that business in the course of its transmission over a telecommunication system.

(2) A person may only intercept an indirect communication in terms of subsection (1) –

(a) if such interception is affected by or with the express consent of the system controller;
(b) for the purposes of –
  (i) monitoring or keeping a record of indirect communications;
    (aa) in order to establish the existence of facts;
    (bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; or
    (cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system;
  (ii) monitoring indirect communication made to a confidential voice telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose;
(c) if the telecommunications system concerned is provided for use wholly or partly in connection with the particular business; and
(d) if the system controller has made all reasonable efforts to inform in advance a person who intends to use the telecommunication system concerned that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses the telecommunication system.

RICA, through section 6, allows an employer to intercept indirect communication (which includes e-mail): provided, however, that an indirect communication that is to be intercepted relates to a transaction entered into in the course of business or it otherwise relates to the business or that the communication otherwise takes place in the ordinary course of business. However, such interceptions may only happen if:

(a) the systems controller[51] had consented thereto, whether expressly or implicitly;

(b) if the monitoring is done with a view of keeping records of indirect communications or if it is for the purpose of investigating or detecting unauthorised use of the telecommunication system[52];

(c) the telecommunications system is used wholly or partly in connection with the particular business; and

(d) the system controller had made all reasonable efforts to inform the person who (intends) using the system that indirect communications may be intercepted with the express or implied consent of the system controller. This "warning" must be given in advance.

This means that an employer may, on prior notice to the employee (and with the employee's consent) monitor e-mail communications sent / received on its network in order to keep records of e-mail transactions. The employee's consent need not be express. For example, if employees are informed that the company intends monitoring e-mail traffic and if the employee does not object to such monitoring the company can lawfully monitor e-mails sent / received. If, on the other hand, the employee does not consent to such monitoring of her/his e-mail, the company cannot monitor her/his e-mail and if it were to found to be in breach of company policy use it in disciplinary proceedings.

4.3 PENALTIES

Failure to comply with section 6(2) is an offence[53]. Upon conviction, a fine not exceeding R2 000 000 or imprisonment not exceeding 10 years may be imposed. It is therefore of the utmost importance to ensure that employers comply with the provisions of section 6.

4.4 THE WAY FORWARD

Companies have a need to ensure that its telecommunications resources are not abused by employees. If undesirable e-mails are sent on the company's domain name it may send out a negative image about the company to the public. For example, a company may be associated with socially unacceptable behaviour or practices, which in turn, may have a negative impact on its client / customer relations. It is an entrenched legal principle that employers can reasonably expect from employees to act in a manner that will not adversely affect the employer.

Over and above the negative impact that an employee's sending of non-work related e-mails may have on the employer, the negative impact on the company's telecommunications system cannot be over-emphasised: abuse of the e-mail system leads to over-trafficking of the network, that slows down the network for business related mail; it leads to lower productivity; increase in costs of maintenance, etc. Moreover, it is a well known fact that a lot of the so-called forwards contain viruses which leads to further losses in terms of down time and corruption of the network. Whichever way one looks at it, an abuse of the company's electronic resources is bad for business.

---

[51] In the case of a juristic person the Chief Executive Officer (or Managing Director) or any other person duly authorised by that officer, e.g. IT Manager.
[52] Section 6(2)(b)(ii) not included for purposes of discussion.
[53] RICA section 51(1)(a).

To this end, the following are recommended to ensure that the business runs effectively but also to ensure compliance with legislation (although it is presently uncertain as to the likely application of section 6 by our Courts):

(a) Prepare a detailed policy regarding the use of company resources. Aspects such as use of the company resources (i.e. only for business, some private use), prohibition on any form of discriminatory e-mails, chain letters, virus warnings, etc. The policy must recognise an employee's right to freedom of expression and right to privacy. However, as neither of these rights are absolutes in the Constitution, they need not be absolutes in the company's policy.

This policy must be linked to the company's disciplinary code.

(b) Inform employees of the policy and provide a time period for comment, whereafter it is implemented. (The policy must contain a clause in terms of which the employee consents to the monitoring of indirect communications).

(c) Redraft all standard letters of appointment in terms of which employees irrevocably consent to the monitoring of indirect communication in accordance with RICA.

(d) Train managers on the policy.

(e) Implement the policy consistently.

5. CONCLUSION

At present there appears to be varying interpretations by our Courts on whether or not the interception of telephone calls breaches an employee's Constitutional right to privacy. The position concerning e-mails is even less certain, although the enactment of RICA brought a measure of clarity.

It would be wise to keep in mind that, although the rights contained in the Bill of Rights are not absolute and may be limited under certain circumstances, the Constitution remains the supreme law of South Africa from which no other law is allowed to deviate. Section 6 of RICA still needs to pass Constitutional muster (probably judged at the hand of the section 36 limitation clause of the Constitution).

It is submitted that this is likely to happen, but even should the monitoring of e-mails in terms of section 6 be found to be unconstitutional, it must be kept in mind that our Courts retain the right to admit evidence obtained in an improper (eg. unconstitutional) manner. It is submitted that he likelihood of a Court accepting such evidence would be higher if the prescriptions of section 6 were followed in a scrupulous manner.

Whatever the likely future interpretation by our Courts of RICA and specifically section 6 thereof, it is therefore submitted that all prudent employers adopt a relevant e-mail policy as suggested above at the workplace.

REFERENCES

CASE LAW

Bernstein and Others v Bester and Others NNO 1992 2 SA 751 (CC).

Case and Another v Minister of Safety and Security and Others 1996 3 SA 617 (CC).

Curtis v Minister of Safety and Security and Others 1996 3 SA 617 (CC).

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

*Moonsamy v the Mailhouse*1999 20 ILJ 464 (CCMA).

National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others 1999 1 SA 6 (CC).

Protea Tech v Weiner 1997 9 BCLR 1225 (W).

S v Bhulwana 1996 1 SA 388 (CC).

S v Jordan and Others (Sex Workers Education and Advocacy Task Force and Others as Amici Curiae) 2002 6 SA 642 (CC).

S v Makwanyane 1995 3 SA 391 (CC).

S v Manamela and Another (Director-General of Justice intervening) 2000 3 SA 1 (CC).

Waste Products Utilisation (Pty) Ltd v Wilkes 2003 2 SA 550 (W)

LEGISLATION

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

Constitution of the Republic of South Africa Act 108 of 1996.

Criminal Procedure Act 51 of 1977.

General Law Amendment Act 62 of 1955

Indecent or Obscene Photographic Matter Act 37 of 1967.

Interception and Monitoring Prohibition Act 127 of 1992.

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

Riotous Assemblies Act 17 of 1956.

Security Officers Act 92 of 1987.

Sexual Offences Act 23 of 1957.

BOOKS AND JOURNALS

De Waal J, Currie I *et al The Bill of Rights Handbook* 1998 Juta.

McQoid-Mason *Constitutional Law of South Africa* 1998 Juta.

Sukhraj P "New Law stops bosses spying on e-mail" *Sunday Times* 2 February 2002 5.