MASERUMULE
Consulting | Learning | Organisational Growth

INTERCEPTION OF ELECTRONIC COMMUNICATIONS BY EMPLOYERS

The Regulation of Interception of Communications and Provision of Communication-related Information Act, Act 70 of 2002 (hereafter the Act) places a general prohibition on intercepting any communication in the course of its occurrence or transmission. Generally speaking, the Act aims to regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information. The Act was promulgated on 30 December 2002 and is expected to come into effect soon. It highlights pertinent issues on monitoring and intercepting employee e-mail and voicemail by employers.

Provision is made for several exceptions to the general prohibition on the interception of communication. Interception is indeed permitted in accordance with an interception direction; by a party to the communication – unless it is interception for purposes of committing an offence; under certain circumstances by law enforcement officers; with the consent of parties to the communication and when the interception occurs in connection with carrying on of business.

"Interception" of communication means the acquisition of the contents of any communication so as to make it available to a person other than the sender or intended recipient. Interception also includes monitoring, inspection of the contents and diversion thereof to any other destination. It is important to note that the observation of communication traffic is not included in the definition of "interception".

"Communication includes direct and indirect communication. The latter specifically refers to the transfer of information in the form of inter alia speech, data, text, visual images, signals and music or other sounds. In the work environment, the interception of e-mail messages, voicemail and so-called sms messages is consequently specifically included in the general prohibition on the interception of communication.

Contravention of the prohibition on interception constitutes an offence that carries a fine of not more than R2 million or imprisonment of not more than 10 years.

One exception to the general prohibition on the interception of communication is dealt with in section 5 of the Act, which states that any person may intercept communication if one of the parties to the communication has given prior written consent to such interception, unless such communication is intercepted by such person for purposes of committing an offence.

Section 6 of the Act provides for a further exception on the general prohibition. In terms of that section, any person may, in the course of carrying on of business, intercept any indirect communication that relates to that business in the course of transmission thereof. More specifically, the section concerned requires that interception may only occur if it has been consented to by the system controller (generally the employer), or if it is done in order to establish the existence of facts, or to investigate the unauthorized use of the system, or where it is undertaken in order to secure the effective operation of the system. Furthermore, the telecommunication system must be provided for use wholly or partly in connection with that business and the system controller must have made all reasonable efforts to inform in advance a person who intends to use the system that communication may be intercepted with the express or implied consent of the person who uses that system.

Recent media reports stated that employers at all times need the written consent of employees to monitor and intercept e-mail communications and have understandably caused concern among employers. The debate centres on the interpretation of two sections of the Act, namely the exceptions to the rule that nobody may intercept another communication – including e-mail, sms, postal and telephone conversations.

In terms of section 5 any person, including an employer, may intercept a communication if one of the parties to the communication has given his or her prior consent to such interception. This does not mean however that this is the only way in which an employer may intercept indirect communication. Section 6 has a more specific application and states that any person in the course of operating any business may intercept any indirect communication if the above requirements are met.

The debate specifically revolves around whether an employer is entitled to intercept an employee's indirect communications without obtaining the employee's prior written consent. Many advisers stated that employers are not entitled to intercept such communications without the prior written consent of the employee. Previous newspaper articles have gone on to state that any employer not meeting the prior written consent requirement will be guilty of an offence and liable to a fine of up to R10 million or to imprisonment of up to 10 years. It is no wonder that these incorrect statements have caused much concern and confusion among employers, especially given the employment law and administrative problems employers would face if they had to amend the employment contracts of all their existing employees.

A careful reading of the sections in question should serve to allay most fears as the requirement for consent to be in writing is contained only in section 5 of the Act, which section is not directly applicable to the interception of communications in connection with carrying on of a business. The latter is governed by section 6 of the Act, which section does not contain a provision that such consent need be in writing. Express or implied consent is merely one of the ways in which an employer could meet the requirements of section 6 of the Act. As pointed out above, section 6 also provides for permission to intercept indirect communication if the system controller has made all reasonable efforts to inform in advance a person who intends to use the telecommunications system concerned that indirect communication transmitted by means thereof, may be intercepted with the express or implied consent of the person who uses that telecommunication system.

It should be evident that an employer may intercept its employees' indirect communications where the employer:

- makes all reasonable efforts to inform the employee, in advance of the employee using the communication system, that the employee's indirect communications may be intercepted; or
- obtains the employee's express consent to the interception of indirect communication; or
- obtains the employee's implied consent to such interception. The relevant section does not acquire consent to be in writing.

The requirements of making reasonable efforts or obtaining express or implied consent presuppose the need for businesses to ensure that the technical or other solutions they choose to implement indeed comply with the legal requirements in question. The requirement of reasonable efforts indicates the need for businesses to ensure that a proper and extensive internal information technology user policy is in place. In the case of implied consent, an employee could, for example, electronically sign a so-called 'click that' agreement in terms of which he will be deemed to have consented to the interception by clicking on the "I accept' button at the time of logging onto the company's network.

Where an employer obtains an employee's prior written consent, the employer would, it seems, be informing the employee in advance that the employee's indirect communications might be intercepted and that it is the intention to do so. The Act does however not require employers to go to these lengths. It is obviously the safest to obtain an employee's prior written consent, as such an employee would not be able to argue that he or she was not aware or did not consent to his or her indirect communications being intercepted.

A further aspect to keep in mind is how and when the employer may gain access to an e-mail message, for example, that have already been transmitted between two parties and that is stored on the recipient's system. In such a case, where transmission has already occurred, interception according to the Act can no longer be effected and the provisions of the Act are not longer applicable. This does not necessarily grant employers free access to the employee's computer where the e-mail is stored. Employers would have to make provision for legal access in this regard and aspects such as privacy rights need to be regulated in internal policies or employment contracts.

The most appropriate steps to be taken by employers to ensure compliance with the Act will depend on the content of each employer's existing employment contracts, e-mail policy and the degree to which e-mail facilities are made available to its employees and for which purposes such facilities are made available.

It should however be remembered that an employee who has Internet access may damage the business in other ways. An employee could, for example, waste time on the Internet or overload the office network with private material. Abuse of this sort can often be detected by observing network traffic. It is not necessary to know the content of, or intercept, communications when observation takes place. Employees may still object to observation but it is easier to justify monitoring traffic than intercepting communications and monitoring traffic does not carry heavy criminal penalties. Observing traffic can also

point to possible cases of serious abuse. This could in turn justify intercepting communications.

Intercepting communications, observing communication traffic and the appropriate use of office communication tools should be dealt with in an office communications policy. Businesses that have to start complying with the legislation on intercepting communications may do well to take this opportunity to revisit their office communication policies.