CHAPTER 11:20

INTERCEPTION OF COMMUNICATIONS ACT

Act 6/2007, 5/2014 (s. 33)

ARRANGEMENT OF SECTIONS

AN ACT to provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of a monitoring centre; and to provide for any other matters connected with or incidental to the foregoing.

[Date of commencement : 3rd August, 2007]

PART I

PRELIMINARY

1 Short title

This Act may be cited as the Interception of Communications Act [*Chapter 11:20*].

2 Interpretation

(1) In this Act—

"access" means the technical ability to interface with a communications facility such as a telecommunications line or switch to enable the interception of any communication carried on at that facility;

"agency" means the government telecommunications agency comprising telecommunications experts which has been designated to operate the monitoring facility and which gives technical directions to service providers so as to ensure compliance with the provisions of this Act;

"Authority" means the Postal and Telecommunications Authority established by section 3 of the Postal and Telecommunications Act [*Chapter 12:05*] (No. 4 of 2000);

"authorised person" means a person referred to in section 5;

"call" means any connection, fixed or temporary, capable of transferring information between two or more users of a telecommunications system;

"call-related information" includes switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment, facility or service provided by a service provider and, where applicable, the location of the user within the telecommunications system;

"customer" means—

(*a*) any person, body or organisation which has entered into a contract with the service provider for the provision of a telecommunication service to that person, body or organisation; or

(*b*) any person to whom or any body or organisation to which a service provider provides a pre-paid telecommunication service;

"detention order", means an order to detain a postal article issued in terms of section 14;

"identity document" has the meaning given to that term by section 32(1) of the Public Order and Security Act [*Chapter 11:17*] (No. 1 of 2002);

"intercept", in relation to any communication which is sent—

(*a*) by means of a telecommunication system or radiocommunication system, means to listen to, record , or copy, whether in whole or in part;

(*b*) by post, means to read or copy the contents, whether in whole or in part;

"interception interface" means the physical location within the service provider's telecommunications facilities where access to the intercepted communication or call-related information is provided;

"interception subject" or "target" means the person whose communications are to be or are being intercepted;

"key" means a numeric code or other means by which information is encrypted;

"Minister" means the Minister of Transport and Communications or any other Minister to whom the President may from time to time assign the administration of this Act;

"monitoring centre" means a central monitoring apparatus designated to be the monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorised person;

"national security of Zimbabwe" includes matters relating to the existence, independence and safety of the State;

"organised criminal group" means a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious offences in order to obtain, directly or indirectly, a financial or other material benefit;

"party", in relation to a communication, means a person whose access to the communication is or might reasonably be known by all other parties;

"protected information" means information that is encrypted by means of a key;

"serious offence" means conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

"service provider" means the provider of a postal service or telecommunication service;

"warrant" means a warrant issued in terms of section 6.

(2) Any word or expression to which a meaning has been assigned in the Postal and Telecommunications Act [*Chapter 12:05*] (No. 4 of 2000) shall have the same meaning when used in this Act.

PART II

CONTROL OF INTERCEPTION AND ESTABLISHMENT OF MONITORING CENTRE

3 Control of interception

(1) Subject to subsection (2), no person shall—

(*a*) intercept any communication in the course of its transmission by means of a telecommunication system or radiocommunication system unless—

(i) he or she is a party to the communication; or

(ii) he or she has the consent of the person to whom, or the person by whom, the communication is sent; or

(iii) he or she is authorised by warrant;

(*b*) intercept any communication in the course of its transmission through the post unless—

(i) he or she has the consent of the person to whom, or the person by whom, the communication is sent; or

(ii) he or she is authorised by warrant.

(2) Subsection (1) shall not apply to the *bona fide* interception of a communication for the purpose of or in connection with the provision, installation, maintenance or repair of a postal, telecommunication or radiocommunication service.

(3) Subject to subsections (1) and (2), any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place, any communication in the course of its occurrence or transmission shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

4 Establishment of monitoring centre

(1) There shall be established a centre to be known as the Monitoring of Interception of Communications Centre (MICC).

(2) The monitoring centre shall be the sole facility through which authorised interceptions shall be effected.

(3) The monitoring centre shall be manned, controlled and operated by technical experts designated by the agency.

(4) The monitoring centre shall give technical advice to—

(*a*) authorised persons; and

(*b*) service providers;

on the interception of communications in terms of this Act.

PART III

APPLICATION FOR LAWFUL INTERCEPTION OF COMMUNICATIONS

5 Authorised persons to apply for warrant of interception

(1) An application for the lawful interception of any communication may be made by the following persons—

(*a*) the Chief of Defence Intelligence or his or her nominee;

(*b*) the Director-General of the President's department responsible for national security or his or her nominee;

(*c*) the Commissioner of the Zimbabwe Republic Police or his or her nominee;

(*d*) the Commissioner General of the Zimbabwe Revenue Authority or his or her nominee.

(2) An application in terms of subsection (1) shall be made by an authorised person to the Minister for the Minister to issue a warrant for the interception of any communication.

(3) An application in terms of subsection (1) shall contain the following information—

(*a*) the person or customer, if known, whose communication is required to be intercepted; and

(*b*) the service provider to whom the direction to intercept the communication must be addressed, if applicable; and

(*c*) the nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and

(*d*) full particulars of all the facts and circumstances alleged by the applicant in support of his or her application; and

(*e*) whether other investigative procedures have been applied and have failed to produce the required evidence, or the reason why other investigative procedures appear to be unlikely to succeed if applied, or whether they involve undue risk to the safety of members of the public or to those wishing to obtain the required evidence:

Provided that this paragraph shall not apply to an application for the issuing of a warrant in respect of a serious offence;

and

(*f*) the period for which the warrant is required to be issued; and

(*g*) the basis for believing that communication relating to the ground on which the application is made will be obtained through the interception; and

(*h*) any other information which may be required by the Minister for the Minister to make an appropriate decision.

6 Issue of warrant

(1) A warrant shall be issued by the Minister to an authorised person referred to in section 5 if there are reasonable grounds for the Minister to believe that—

(*a*) any of the following offences has been or is being or will probably be committed—

(i) a serious offence by an organised criminal group; or

(ii) an offence referred to in the Third Schedule or in paragraph 1, 2, 3, 4, 5, 6, 7 or 8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*];

(*b*) the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary; or

(*c*) the gathering of information concerning a potential threat to public safety or national security is necessary.

(2) The Minister may, if he or she is of the opinion that the circumstances so require—

(*a*) upon an application being made in terms of this Part, issue instead of a warrant any directive to a service provider not involving any interception or monitoring of communications; or

(*b*) after a warrant has been issued, amend or revoke the warrant.

7 Scope of warrant and renewal thereof

(1) A warrant shall—

(*a*) subject to subsection (2), be valid for such period not exceeding three months as may be specified therein but may, for good cause shown by the authorised person, be renewed for a period not exceeding three months—

(i) by the Minister in respect of a serious offence by an organised criminal group or for a purpose specified in section 6(1)(*b*) or (*c*);

(ii) by the Minister in consultation with the Prosecutor-General in respect of an offence referred to in the Third Schedule or in paragraph 1, 2, 3, 4, 5, 6, 7 or 8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*];

(*b*) specify the name and address of the interception subject and the manner of interception;

(*c*) order the service provider to strictly comply with such technical requirements as may be specified by the agency to facilitate the interception;

(*d*) specify the apparatus and other means that are to be used for identifying the communication that is to be intercepted;

(*e*) contain any other necessary details relating to the interception target.

(2) Upon expiry of a warrant that is renewed in terms of subsection (1)(*a*)(i) or (ii) within six months of such expiry, the warrant may, for good cause shown by the authorised person, be renewed for a further period not exceeding three months—

(*a*) by the Minister in consultation with the Prosecutor-General in respect of a serious offence by an organised criminal group or for a purpose specified in section 6(1)(*b*) or (*c*);

(*b*) by the Administrative Court upon an *ex parte* application by the authorised person concerned, in respect of an offence referred to in the Third Schedule or in paragraph 1, 2, 3, 4, 5, 6, 7 or 8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*].

(3) Upon expiry of a warrant that is renewed in terms of subsection (2)(*b*) or within six months of such expiry, the warrant may, for good cause shown by the authorised person, be renewed for a further period not exceeding three months by the Administrative Court upon an *ex parte* application by the authorised person concerned.

(4) Every renewal of a warrant that is sought within six months of the expiry of a warrant that was renewed in terms of subsection (2)(*a*) or (3) or this subsection may be renewed for further periods not exceeding three months at a time by the Administrative Court upon an *ex parte* application by the authorised person concerned.

(5) An authorised person shall notify the Minister in advance and in writing of any application for the renewal of a warrant in terms of subsection (2)(*b*), (3) or (4).".

8 Evidence obtained by unlawful interception not admissible in criminal proceedings

Evidence which has been obtained by means of any interception committed in contravention of this Act shall not be admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave the court shall have regard, among other things, to the circumstances in which it was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused that may be occasioned by its admission or exclusion.

9 Assistance by service providers

(1) A service provider must ensure that—

(*a*) its postal or telecommunications systems are technically capable of supporting lawful interceptions at all times in accordance with section 12;
(*b*) it installs hardware and software facilities and devices to enable interception of communications at all times or when so required, as the case may be;
(*c*) its services are capable of rendering real time and full time monitoring facilities for the interception of communications;
(*d*) all call-relation information is provided in real-time or as soon as possible upon call termination;
(*e*) it provides one or more interfaces from which the intercepted communication shall be transmitted to the monitoring centre;
(*f*) intercepted communications are transmitted to the monitoring centre via fixed or switched connections, as may be specified by the agency;
(*g*) it provides access to all interception subjects operating temporarily or permanently within their communications systems, and, where the interception subject may be using features to divert calls to other service providers or terminal equipment, access to such other providers or equipment;
(*h*) it provides, where necessary, the capacity to implement a number of simultaneous interceptions in order—
(i) to allow monitoring by more than one authorised person;
(ii) to safeguard the identities of monitoring agents and ensure the confidentiality of the investigations;
(*i*) all interceptions are implemented in such a manner that neither the interception target nor any other unauthorised person is aware of any changes made to fulfill the warrant.

(2) A service provider who fails to give assistance in terms of this section shall be guilty of an offence and liable to a fine not exceeding level twelve or to imprisonment for a period not exceeding three years or to both such fine and such imprisonment.

10 Duties of telecommunication service provider in relation to customer

(1) Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, it must obtain—
(*a*) the person's full name, residential address, business address and postal address and his or her identity number contained in his or her identity document;
(*b*) in the case where the person is a business organisation, its business name and address and the manner in which it is incorporated or registered;
(*c*) any other information which the telecommunication service provider deems necessary for the purpose of enabling it to comply with this Act.

(2) A telecommunication service provider must ensure that proper records are kept of the information referred to in subsection (1) and any change in such information.

11 Notice of disclosure of protected information

(1) If an authorised person believes on reasonable grounds—
(*a*) that a key to any protected information is in the possession of any person; and
(*b*) that the imposition of a disclosure requirement in respect of the protected information is necessary—
(i) in the interests of national security; or
(ii) for the purpose of preventing and detecting a serious offence; or
(iii) in the interests of the economic well-being of Zimbabwe;
and
(*c*) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition; and
(*d*) that it is not reasonably practicable for the authorised person to obtain possession of the protected information in an intelligible form without giving the notice under this section;
the authorised person may by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(2) A notice under this section imposing a disclosure requirement in respect of any protected information must—
(*a*) be in writing; and
(*b*) describe the protected information to which the notice relates; and
(*c*) specify why the protected information is required; and
(*d*) specify a reasonable time by which the notice is to be complied with; and
(*e*) set out the disclosure that is required by the notice and the form and manner in which it is to be made.

(3) A notice under this section shall not require the making of any disclosure to any person other than—
(*a*) the person giving the notice; or
(*b*) such other person as may be identified in or under the notice.

(4) A person to whom a notice has been given in terms of this section and who is in possession of both the protected information and the key thereto must—

(*a*) use any key in his or her possession to provide access to the information;

(*b*) in providing such information, make a disclosure of the information in an intelligible form.

(5) If a person to whom a notice has been given is in possession of different keys, or combinations of keys to the protected information—

(*a*) it shall not be necessary for purposes of complying with the notice for the person given notice to disclose any keys in addition to those the disclosure of which , alone, are sufficient to enable the authorised person to obtain access to the protected information and to put it in an intelligible form;

(*b*) the person given notice may select which of the keys or combination of keys may be used for complying with the notice.

(6) If a person to whom a notice has been given—

(*a*) has been in possession of any key to the protected information , but no longer possesses it; and

(*b*) has information that will facilitate the obtaining or discovery of the key to protected information;

he or she must disclose the information referred to in paragraph (*b*) to the authorised person.

(7) An authorised person to whom a key has been disclosed under this section must—

(*a*) use the key only in respect of the protected information, and in the manner and for the purposes specified in the notice; and

(*b*) on or before the expiry of the period or extended period for which the notice has been issued, destroy all records of the disclosed key if, in the opinion of the authorised person—

(i) no criminal proceedings or civil proceedings will be instituted in connection with such records; or

(ii) such records will not be required for any criminal or civil proceedings.

(8) A person who fails to make the disclosure required by the notice issued under this section shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

12 Interception capability of telecommunication service

(1) Notwithstanding any other law, a telecommunication service provider shall—

(*a*) provide a telecommunication service which has the capability to be intercepted; and

(*b*) store call-related information in accordance with a directive issued under subsection (2).

(2) The Authority shall, after consultation with the Minister, within two months and after the date of commencement of this Act, issue a directive to telecommunication service providers specifying—

(*a*) the manner in which effect is to be given to subsection (1) by every telecommunication service provider; and

(*b*) the security, technical and functional features of the facilities and devices to be acquired by every telecommunication service provider to enable—

(i) the interception of communication in terms of this Act; and

(ii) the storing of call-related information; and

(*c*) the period within which the directive must be complied with.

(3) A directive referred to in subsection (2) must specify—

(*a*) the capacity and technical features of the devices or systems to be used for interception purposes;

(*b*) the connectivity of the devices or systems to be used for interception purposes with the monitoring centre;

(*c*) the manner of routing intercepted information to the monitoring centre;

(*d*) any other relevant matter which the Authority deems necessary or expedient.

(4) A telecommunication service provider shall, at his or her own expense, acquire the facilities and devices specified in a directive issued in terms of subsection (2).

(5) Subject to section 13, any cost incurred by a telecommunication service provider under this Act for the purpose of—

(*a*) enabling—

(i) a telecommunication service to be intercepted; and

(ii) call-related information to be stored;

and

(*b*) complying with section 9;

shall be borne by the telecommunication service provider.

13 Compensation payable to service provider or protected information key holder

(1) The Minister, after consultation with the Authority, shall by notice in the *Gazette* prescribe—

(*a*) the forms of assistance given by a service provider or protected information key holder in the execution of a warrant, notice or directive issued in terms of this Act for which it must be compensated by the State; and

(*b*) reasonable tariffs of compensation payable to a service provider or protected information key holder for providing the forms of the assistance referred to in paragraph (*a*).

(2) The forms of assistance referred to in subsection (1)(*a*) must include , in the case of—

(*a*) a telecommunication service provider, the making available of a facility, device or telecommunication system; and

(*b*) a protected information key holder—

(i) the disclosure of the key; and

(ii) the provision of assistance in rendering intelligible the protected information.

(3) The tariffs prescribed under subsection (1)(*b*)—

(*a*) may differ in respect of different categories of service providers, or protected information key holders;

(*b*) must be uniform in respect of each service provider or protected information key holder falling within the same category.

(4) The compensation payable to a service provider or protected information key holder shall only be for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance referred to in subsection (1)(*a*).

PART IV

POSTAL ARTICLES

14 Application for detention order

(1) If an authorised person suspects on reasonable grounds that a postal article in the custody of a postal service provider—

(*a*) contains anything in respect of which an offence or attempted offence is being committed; or

(*b*) contains anything that will afford evidence of the commission of an offence; or

(*c*) is being sent to further the commission of an offence; or

(*d*) needs to be obtained and examined in the interests of defence, public safety or public order;

he or she may apply to the Minister for a detention order to detain the postal article for the purpose of examination.

(2) If the Minister, by written order to the authorised person and the postal service provider, certifies that it is necessary for any of the purposes specified in subsection (1)(*a*), (*b*), (*c*) or (*d*) for a postal article in the postal service provider's custody to be detained and, if so required by the order, opened and examined, the postal service provider shall forthwith detain the postal article.

(3) Section 5 shall apply with such changes as may be necessary to the information required to be furnished to the Minister before a detention order is issued.

15 Examination of and accountability for detained postal articles

(1) On the day appointed by or under a detention order the authorised person shall, in the presence of a representative of the postal service provider, examine the detained postal article.

(2) If, on examination of a postal article in terms of subsection (1), the suspicion that gave rise to its examination—

(*a*) is substantiated, the postal article may be detained for the purposes of evidence in a criminal prosecution or destroyed or dealt with in such other manner as may be authorised in the detention order;

(*b*) is not substantiated, the postal article shall be delivered to the person to whom it is addressed or to his or her representative on payment of any postage payable thereon.

PART V

GENERAL

16 Restriction on disclosure

(1) No person may disclose any communication or information which he or she obtained in the exercise of his or her powers or the performance of his or her duties in terms of this Act except—

(*a*) to any other person who of necessity requires it for the like exercise or performance of his or her functions in terms of this Act;

(*b*) information which is required to be disclosed in terms of any law or as evidence in any court of law.

(2) No—

(*a*) service provider or protected information key holder may disclose any information which it obtained in compliance with this Act; or

(*b*) employee of a service provider or protected information key holder may disclose any information which he or she obtained in the course of his or her employment and which is connected with the exercise of any power or the performance of any duty in terms of this Act.

(3) Any person who discloses any information in contravention of subsection (1) or (2) shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

17 Disposal of intercept product

Subject to sections 11(7)(*b*) and 15(2), an authorised person shall destroy as soon as possible after it is used for the purposes of this Act any intercepted communication.

18 Appeals

(1) Any person who is aggrieved by a warrant, a directive referred to in section 6(2)(*a*) or a directive or order issued to or by the Authority, an authorised person or the agency may appeal to the Administrative Court within one month of being notified or becoming aware of it, as the case may be.

(2) The Administrative Court may in any appeal confirm, vary or set aside the warrant, directive or order appealed against and may make such order as to costs as it thinks fit.

(3) For the avoidance of doubt, the Administrative Court is an "adjudicating authority" for the purposes of the Courts and Adjudicating Authorities (Publicity Restriction) Act [*Chapter 7:04*] when considering any appeal in terms of this section.

19 Review of exercise of Minister's powers under this Act

(1) No later than three months after the end of each calendar year the Minister shall submit for review by the Prosecutor-General a written summary of the particulars of every warrant which, during that calendar year, was issued by him or her but not renewed in terms of section 7(1)(*a*)(i) or (ii), (2), (3) or (4).

(2) On receiving the summary referred to in subsection (2) the Prosecutor-General may request further particulars in relation to any warrant mentioned in the summary, and the Minister shall comply as soon as practicable with any such request.

(3) Upon reviewing the summary referred to in subsection (2), together with any further particulars provided in compliance with subsection (3), the Prosecutor-General may make recommendations in writing to the Minister concerning the manner in which the Minister shall exercise his or her powers in future generally or with respect to the issuance of any class of warrant, and the Minister shall comply with such recommendations.

20 Regulations

The Minister may make regulations providing for all matters which by this Act are required or permitted to be prescribed or which, in his or her opinion, are necessary or convenient to be prescribed for carrying out or giving effect to this Act.