



REPUBLIC OF BOTSWANA

GOVERNMENT GAZETTE EXTRAORDINARY

Vol. LX, No. 3

GABORONE

12th January, 2022

CONTENTS

Page

| | |
|--|----------|
| Supplement B — Criminal Procedure and Evidence (Controlled Investigations) Bill, 2022 – Bill No. 1 of 2021..... | B.1 – 16 |
|--|----------|

The Botswana Government *Gazette* is printed by Department of Government Printing and Publishing Services, Private Bag 0081, GABORONE, Republic of Botswana. Annual subscription rates are P600,00 post free surface mail, SADC Countries airmail P1,357,00, Rest of Africa airmail P1,357,00, Europe and USA airmail P1,735,00.

The price for this issue of the Extraordinary *Gazette* is P1.00.

Bill No. 1 of 2022

**CRIMINAL PROCEDURE AND EVIDENCE (CONTROLLED
INVESTIGATIONS) BILL, 2022**

(Published on 12th January, 2022)

MEMORANDUM

1. A draft of the above Bill, which is intended to be presented to the National Assembly, is set out below.

2. The object of the Bill is to enact the Criminal Procedure and Evidence (Controlled Investigations) Bill to make provision for controlled investigations and an undercover operations framework, including the handling of information by investigatory authorities.

3. Part I provides for the preliminary provisions. Part II provides for an undercover operations framework and formalises the collection of information through undercover operation orders and assumed identities. It allows the Registrar of Births and Deaths, the Registrar of National Registration and the Registrar of Marriages to make entries into their registers by order of the court for purposes of controlled investigations. It further makes provision for travel documents to be issued under assumed identities.

4. Part III provides for an interception of communications framework, which authorises the interception of communications by investigatory authorities and sets out the role of service providers in controlled investigations for the gathering of criminal evidence.

5. Part IV introduces provisions for the handling of information in controlled investigations. Part V broadens the scope of admissible evidence to include information gathered in controlled investigations. Part VI provides for miscellaneous provisions, which include the legal immunity of staff of an investigating authority, as well as the regulation-making powers of the Minister.

KAGISO THOMAS MMUSI,
Minister of Defence, Justice and Security.

ARRANGEMENT OF SECTIONS

SECTION

PART I — *Preliminary*

1. Short title and commencement
2. Interpretation
3. Jurisdiction

PART II — *Undercover Operations*

4. Undercover operation without warrant
5. Application for undercover operation warrant
6. Determination of undercover operation warrant
7. Joint undercover operation
8. Application for assumed identity
9. Authorisation for assumed identity
10. Issuance of assumed identity
11. Variation or cancellation of authority
12. Annual review of issued authorities
13. Entries in the registers
14. Cancellation of authority for registers
15. Prohibition of disclosure of identity

PART III — *Interception of Communications*

16. Interception of communications without warrant
17. Application for interception warrant
18. Control of interception
19. Determination for interception warrant
20. Issuance of interception warrant
21. Evidence obtained in excess of authorisation or warrant
22. Notice of disclosure of protected information
23. Restriction on disclosure of communication or information
24. Duties and responsibilities of service providers

PART IV — *Handling of Information from Controlled Investigations*

25. Handling of information
26. Retention and storage of information
27. Retention of electronic record

PART V — *Admissibility of Evidence*

28. Legally obtained information
29. Evidence relating to carrying out of controlled investigation

- 30. Admissibility of evidence from foreign State
- 31. Inadmissible evidence

PART VI — *Miscellaneous Provisions*

- 32. Legal indemnity
- 33. Offences and penalties
- 34. Regulations

A Bill
—entitled—

An Act to provide for the authorisation of investigations for purposes of controlled investigations and the gathering of criminal evidence within and outside Botswana and to provide for any other related matters.

Date of Assent:

Date of Commencement:

ENACTED by the Parliament of Botswana.

PART I — *Preliminary (ss 1-3)*

1. This Act may be cited as the Criminal Procedure and Evidence (Controlled Investigations) Bill, 2022, and shall come into operation on such date as the Minister may, by Order published in the *Gazette*, appoint. Short title and commencement

2. In this Act, unless the context otherwise requires — Interpretation

“applicant” means a law enforcement officer in an investigatory authority who applies for a warrant or an order under this Act;

“Authority” means the Communications Regulatory Authority;

“communication service” has the same meaning assigned to it under the Communications Regulatory Authority Act; Cap. 72:03

“comparable body” means an institution or government agency outside Botswana with functions similar to those of an investigatory authority;

“controlled delivery” means the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, —

(a) with the knowledge and under the supervision of their competent authorities; and

(b) for the purpose of —

(i) the investigation of an offence, and

(ii) the identification of persons involved in the commission of the offence;

“controlled investigation” include —

(a) undercover operations; and

(b) the interception of communications;

B.4

- Cap. 08:02 “court” or “the court” has the same meaning assigned to it under the Criminal Procedure and Evidence Act;
- “informant” means a person who provides useful and credible information regarding criminal activity or a matter of interest to an investigatory authority, and includes —
- (a) a member of the public;
 - (b) the victim of a crime;
 - (c) a member of an organised criminal group; and
 - (d) an investigating officer;
- “intercept” means aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make the contents of a communication available to a person other than the sender or the recipient or intended recipient of that communication, and includes the —
- (a) monitoring of communication by means of a monitoring device;
 - (b) viewing, examination or inspection of the contents of any communication; and
 - (c) diversion of any communication from its intended destination to any other destination;
- “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” means the person whose communications are to be or are being intercepted;
- “investigating officer” means an investigator in an investigatory authority;
- Cap. 08:07 “investigatory authority” has the same meaning assigned to it under the Financial Intelligence Act;
- “judicial officer” has the same meaning assigned to it under the Criminal Procedure and Evidence Act;
- “key” means a numeric code or other means by which information is encrypted;
- Cap. 08:03 “serious crime related activity” has the same meaning assigned to it under the Proceeds and Instruments of Crime Act;
- “service provider” has the same meaning assigned to it under the Communications Regulatory Authority Act; and
- “target” means a person, place, vehicle, receptacle or anything in respect of which a controlled investigation has been authorised.
- Jurisdiction **3.** (1) The courts of Botswana shall have jurisdiction where an act done or an omission made constituting an offence under this Act has been committed —
- (a) in the territory of Botswana;

- (b) by a national of Botswana outside the territory of Botswana, if the person's conduct constitutes an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country;
- (c) on a ship or aircraft registered in Botswana;
- (d) in part in Botswana; or
- (e) outside the territory of Botswana and where any result of the offence has an effect in Botswana.

PART II — *Undercover Operations (ss 4-15)*

4. (1) Where a head of an investigatory authority believes, on reasonable grounds, that the delay in obtaining an undercover warrant would defeat the object of the undercover operation, he or she may, in writing, authorise an investigating officer to engage in an undercover operation to detect, investigate or uncover the commission of an offence, or to prevent the commission of any offence.

Undercover
operation
without
warrant

(2) An authorisation issued under subsection (1) shall not be for a period exceeding 14 days.

5. (1) An investigating officer shall make an *ex parte* application to the court for an undercover operation warrant for purposes of gathering evidence in a controlled investigation.

Application
for undercover
operation
warrant

(2) An *ex parte* application under subsection (1) shall be heard in camera.

(3) A warrant issued under subsection (1) shall be in writing and specify —

- (a) the date and time of the signing, and the time from which the approval takes effect;
- (b) the persons who are authorised to participate in the operations;
- (c) the nature of the conduct in which the participants are authorised to engage, including —
 - (i) covert operations;
 - (ii) use of informants; and
 - (iii) controlled delivery;
- (d) the jurisdiction where the warrant is enforceable; and
- (e) a period, not exceeding three months, for which the approval is given.

6. (1) A court may grant an application to carry out an undercover operation for the purposes of gathering evidence of serious crime related activities where the court is satisfied that —

Determination
of undercover
operation
warrant

- (a) a person has engaged, is engaging or is about to engage in serious crime related activities of the kind to which the proposed undercover operation relates;
- (b) the proposed undercover operation is not more extensive than could reasonably be justified in view of the nature and extent of the suspected serious crime related activity;

B.6

(c) the means are proportionate to the proposed undercover operation and are justified by the social harm of the serious crime related activity against which they are directed;

(d) the undercover operation is sufficiently designed to provide a person who has engaged, or is engaging or is about to engage in serious crime related activity an opportunity —

(i) to manifest that behaviour, or

(ii) to provide additional evidence of that behaviour,

without undue risk that persons without a predisposition to a serious crime related activity will be encouraged into a serious crime related activity that they would otherwise have avoided.

(2) In determining an application for an undercover operation, a court shall consider whether approval for similar operations has previously been sought, and, if sought and refused, the reasons for that refusal.

(3) The court may renew, from time to time, a warrant for a period not exceeding 12 months.

Joint
undercover
operation

7. (1) An undercover operation may be conducted jointly by two or more investigatory authorities or agencies.

(2) An investigatory authority that directs and controls an undercover operation under subsection (1) that wishes to engage a non-law enforcement entity shall apply for authority from the Minister to engage such non-law enforcement entity to carry out an undercover activity or use such entity as it considers necessary.

(3) Where a person from another law enforcement agency participates in a joint undercover operation he or she shall conform to the guidance of the investigatory authority that directs and controls the operation, without prejudice to the generality of his or her duties in his or her agency.

Application for
assumed
identity

8. (1) An applicant may apply to the court for authority to acquire an assumed identity for an undercover operation.

(2) An assumed identity application under subsection (1) shall be in writing and shall contain —

(a) the name of the applicant;

(b) where the application is not made by the applicant, the name of the person to be authorised to acquire an assumed identity;

(c) if the authorised person is not a law enforcement officer the name and position of an investigating officer to be appointed as a supervisor of the authorised person during an undercover operation;

(d) the reason for the assumed identity;

(e) details of the investigation or intelligence gathering exercise in respect of which the assumed identity will be used; and

(f) details of the investigatory authority and the type of evidence to be gathered.

Authorisation
for assumed
identity

9. (1) The court may, on receipt of an application under section 8, issue the applicant with an authority to acquire an assumed identity where the court is satisfied that —

- (a) the assumed identity is necessary for purposes of an investigation or intelligence gathering in relation to a serious crime related activity; and
 - (b) the risk of abuse of the assumed identity by the authorised person is minimal.
- (2) An investigating officer appointed as supervisor under section 8 (2) (c) shall hold a designation as may be prescribed.
- (3) A person shall apply for a separate authority for each assumed identity.

10. (1) Where a court issues an authority to acquire an assumed identity under section 9 (1), such authority shall be in writing.

Issuance of assumed identity

- (2) The authority under subsection (1) shall specify —
- (a) the particulars of the person issuing the authority;
 - (b) the date on which the authority comes into effect;
 - (c) details of the assumed identity authorised;
 - (d) details of the evidence to be acquired under the authority;
 - (e) the conditions to which the authority is subject;
 - (f) the reason why the authority is granted;
 - (g) where the authority relates to an applicant, the name of the applicant;
 - (h) where the authority relates to an authorised civilian —
 - (i) the name of the authorised civilian,
 - (ii) the name of his or her supervisor, and
 - (iii) a period which may not exceed three months;
 - (i) whether it authorises an application for an order for —
 - (i) an entry in the register of births and deaths,
 - (ii) an entry in the register of marriages,
 - (iii) the issuance of a travel document, or
 - (iv) an entry in a corresponding law; and
 - (j) the participating jurisdictions in which the assumed identity may be used.

11. (1) An applicant may make an application to a court to vary or cancel an authority.

Variation and cancellation of authority

- (2) Subject to subsection (1), the court —
- (a) may vary or cancel the authority; and
 - (b) shall cancel the authority if satisfied, on a review or otherwise, that the grounds for the granting of the authority no longer exist.
- (3) The court shall give written notice of the variation or cancellation under this section to —
- (a) the applicant; and
 - (b) if the authorised person is an authorised civilian, the authorised person's supervisor.
- (4) The notice under subsection (3) shall specify the reason for the variation or cancellation.
- (5) A variation or cancellation under this section shall take effect on —
- (a) the day the written notice is given to the authorised person; or
 - (b) a specified day in the notice.

B.8

Annual review
of issued
authorities

12. (1) The court shall, at least once in every 12 months' period, review each authority granted under this Part.

(2) Where upon review under subsection (1), the court is satisfied that the grounds for the granting of the authority still exist, the court shall —

- (a) record its opinion and its reasons, in writing; and
- (b) extend the authority.

Entries in the
registers

13. (1) In issuing an applicant with an authority to acquire an assumed identity under subsection (1), the court may authorise the following —

Cap. 30:01

(a) an order for an entry in the register of births and deaths in terms of section 4 of the Births and Death Registration Act;

Cap. 01:02

(b) an order for an entry in the national register in terms of the National Registration Act;

Cap. 29:01

(c) an order for the entry in the register of marriages in terms of section 28 of the Marriage Act;

Cap. 25:02

(d) an order for the issuance of a travel document in terms of the Immigration Act; and

(e) the use of an assumed identity in a participating jurisdiction in which the assumed identity may be used.

(2) Subject to subsection (1), where the court grants an authority it shall order —

(a) the Registrar of Births and Deaths to make an entry in the register under the Births and Deaths Registration Act;

(b) the Registrar of National Registration to make an entry in the register under the National Registration Act;

(c) the Registrar of Marriages to make an entry in the marriage register under the Marriage Act; and

(d) the Director of Immigration to issue a travel document under the Immigration Act,

in relation to the acquisition of an assumed identity under an investigatory authority or comparable body.

(3) The court may make an order under this section —

(a) on application by an applicant; and

(b) where it is satisfied that the order is justified, having regard to the nature of the activities undertaken or to be undertaken by the applicant or person under an investigatory authority or comparable body.

(4) The Registrar of Births and Deaths, the Register of National Registration, the Registrar of Marriages and the Director of Immigration shall give effect to an order under this section —

(a) within the period specified in the order; or

(b) if no period is specified in the order, within 14 days after the day on which the order is made.

Cancellation
of authority in
registers

14. (1) This section shall apply if —

(a) the court cancels an authority for an assumed identity; and

(b) there is an entry in relation to that identity —

- (i) in the register under the Births and Deaths Act, in the register under the National Registration Act, in the register under the Marriages Act or in a travel document issued under the Immigration Act as a consequence of an order under section 12, or
 - (ii) in a register of births, deaths, national registration, marriages or the issuance of a travel document in a participating jurisdiction as a consequence of an order under the corresponding law of the jurisdiction.
- (2) Where subsection (1) (b) (i) applies —
- (a) an applicant shall, within 28 days after the day on which the authority is cancelled, apply to the court for an order that the Registrar of Births, and Deaths, Registrar of National Registration, the Registrar of Marriages or the Director of Immigration cancel the entry; and
 - (b) the Registrar of Births and Deaths, Registrar of National Registration, Registrar of Marriages or the Director of Immigration shall give effect to the order within 28 days after the day on which the order is made.
- (3) Where subsection (1) (b) (ii) applies, the applicant shall apply for an order under the corresponding law to cancel the authority.

Prohibition of disclosure of identity

15. Notwithstanding the provisions of section 8, a person who discloses the identity of another person which he or she obtained or to which he or she has had access by virtue of —

- (a) the performance of his or her duties or functions under this Act; or
- (b) his or her position as a person who holds or has held office in the investigatory authority, and from which the identity of a person who —
 - (i) is or was a confidential source of information to the investigatory authority, or
 - (ii) is or was an officer or support staff engaged in undercover operational activities of an investigatory authority,

can be inferred, and who discloses such information to a person other than a person to whom he or she is authorised to disclose the information to or to whom it may lawfully be disclosed, commits an offence and is liable to a fine not exceeding P50 000 or a term of imprisonment not exceeding 12 years.

PART III — *Interception of Communications (ss 16-24)*

16. (1) Where a head of an investigatory authority believes on reasonable grounds that the delay in obtaining an interception warrant would defeat the object of the investigations, he or she may, in writing, authorise an investigating officer to intercept communications to detect, investigate or uncover the commission of an offence, or to prevent the commission of any offence.

(2) An authorisation made in subsection (2) shall be for a period not exceeding 14 days.

Interception of communications without warrant

B.10

Application
for interception
warrant

17. (1) An applicant shall make an ex parte application to the court for an interception warrant for purposes of gathering evidence in a controlled investigation.

(2) An application under subsection (1) shall contain the following information —

- (a) the person whose communication is intercepted;
- (b) the basis for believing that communication relating to the ground on which the application is made will be obtained through the interception;
- (c) the service provider to whom the direction to intercept the communication shall be addressed, where applicable;
- (d) the nature and location of the place from which the communication is to be intercepted;
- (e) full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;
- (f) whether other investigative procedures have been applied and have failed to produce the required evidence;
- (g) whether other investigative procedures involve undue risk to the safety of members of the public or to those wishing to obtain the required evidence; and
- (h) the period for which the authorisation is required to be issued.

Control of
interception

18. (1) A person shall intercept communication in the course of its transmission —

- (a) by means of a telecommunication system or radio communication system, unless the person —
 - (i) is a party to the communication,
 - (ii) has the consent of the parties to the communication, or
 - (iii) is authorised by warrant, and
- (b) through the post, unless the person —
 - (i) has the consent of the person to whom, or the person by whom, the communication is sent, or
 - (ii) 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 radio communication service.

(3) Subject to subsections (1) and (2), a person who intentionally intercepts or attempts to intercept, or authorises or procures another person to intercept or attempt to intercept, at any place, communication in the course of its occurrence or transmission commits an offence and is liable to a fine not exceeding P50 000 or to a term of imprisonment not exceeding 12 years, or to both.

Determination
for interception
warrant

19. (1) The court shall grant an application to carry out an interception of communication warrant for purposes of gathering evidence of a serious crime related activity where the court is satisfied that there are reasonable grounds to believe that material information relating to —

- (a) the commission of an offence under this Act; or
 - (b) the whereabouts of a person suspected to have committed an offence, is contained in the communication.
- (2) A court may approve a warrant under subsection (1) and may —
- (i) require a communication service provider to intercept and retain specified communication of a specified description received or transmitted, or about to be received or transmitted by that communication service provider, or
 - (ii) authorise an investigating officer to enter a premises and to install on such premises, a device for the interception and retention of a specified communication or other communication of a specified description, and to remove and retain such device.

20. (1) The court may grant a warrant to carry out an interception of communications for purposes of gathering evidence of serious crime related activities where the court is satisfied that —

Issuance of
interception
warrant

- (a) a serious crime related activity is being or will probably be committed;
- (b) the gathering of information concerning an actual threat to national security or to 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) A warrant granted under subsection (1), —

- (a) shall be valid for such period not exceeding three months and may be renewed for a period not exceeding three months;
- (b) shall specify the name and address of the interception subject and the manner of interception;
- (c) may order the service provider to comply with such technical requirements as may be specified by the court to facilitate the interception;
- (d) shall specify the apparatus and other means that are to be used for identifying the communication that is to be intercepted; and
- (e) shall contain any other necessary details relating to the interception target.

(3) The court may, if it is of the opinion that the circumstances so require, amend or revoke the authorisation at any time.

21. (1) Any evidence obtained by means of an interception made in excess of an authorisation or warrant issued under this Part shall be admissible in evidence, in criminal proceedings, only with the leave of the court.

Evidence
obtained in
excess of
authorisation
or warrant

(2) The court in granting or refusing a leave under subsection (1), shall have regard to —

- (a) the circumstances in which the evidence was obtained;
- (b) the potential effect of the evidence admission or exclusion on issues of national security; and
- (c) the unfairness to the accused that may be occasioned by the evidence admission or exclusion.

B.12

Notice of disclosure of protected information

22. (1) Where an applicant has reasonable grounds —
- (a) that a key to protected information is in the possession of a person;
 - (b) that the imposition of a disclosure requirement in respect of protected information is necessary —
 - (i) in the interests of national security,
 - (ii) for the purpose of preventing and detecting a serious crime related activity, or
 - (iii) in the public interest; and
 - (c) that the imposition of a disclosure requirement referred to in paragraph (b) is proportionate to what the imposition seeks to achieve; and
 - (d) that it is not reasonably practicable for the applicant to obtain possession of protected information in an intelligible form without giving of notice under this section,
- the applicant 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 protected information shall —
- (a) be in writing;
 - (b) describe the protected information to which the notice relates;
 - (c) specify why the protected information is required;
 - (d) specify the duration of the notice; 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 disclosure to a person other than —
- (a) the person giving the notice; or
 - (b) such other person as may be specified in 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 shall —
- (a) use the key in his or her possession to provide access to the information; and
 - (b) in providing access to such information, make a disclosure of the information.
- (5) Where a person to whom the notice has been given under this section is in possession of different keys, or a combination of keys, to protected information —
- (a) it shall not be necessary for purposes of complying with the notice for the person given notice, to disclose keys in addition to those the disclosure of which alone, are sufficient to enable the applicant to obtain access to the protected information and to put it in an intelligible form; and
 - (b) the person given notice may select which of the keys or combination of keys, may be used for complying with the notice.

(6) Where a person to whom a notice has been given under this section —

- (a) no longer possesses a key to the protected information; and
- (b) has information that will facilitate the obtaining or discovery of the key to protected information,

he or she shall disclose this, as soon as practicably possible, to the applicant.

(7) The applicant to whom a key has been disclosed under this section shall —

- (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 applicant —

- (i) criminal proceedings or civil proceedings are not being instituted in connection with such records, or
- (ii) such records will not be required for criminal or civil proceedings.

(8) A person who fails to make a disclosure required by the notice issued under this section commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a period not exceeding six years, or to both.

23. (1) A person shall not disclose 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 unless he or she is required to do so in terms of any written law or by an order of the court.

Restriction on disclosure of communication or information

(2) Notwithstanding subsection (1), a person may disclose communication or information 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, —

- (a) to another person who of necessity requires it for the like exercise or performance of his or her functions in terms of this Act; or
- (b) information which is required to be disclosed as evidence in court.

(3) A person who discloses communication or information in contravention of subsection (1) commits an offence and is liable to a fine of not exceeding P50 000 or to imprisonment for a period not exceeding 12 years, or to both.

24. (1) A service provider shall —

- (a) have postal or telecommunications systems which are technically capable of supporting lawful interceptions at all times in accordance with sections 16 and 18;
- (b) install hardware and software facilities and devices which enable the interception of communications at all times or when so required, as the case may be;
- (c) have services which are capable of rendering real time and full time monitoring facilities for the interception of communications;

Duties and Responsibilities of service providers

B.14

- (d) provide all call-related information in real-time or as soon as possible upon call termination;
- (e) provide one or more interception interfaces from which the intercepted communication shall be transmitted to the investigatory authority;
- (f) transmit intercepted communications to the investigatory via fixed or switched connections, as may be specified by the court;
- (g) provide 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) provide, where necessary, the capacity to implement a number of simultaneous interceptions in order to —
 - (i) allow monitoring by more than one authorised person, and
 - (ii) safeguard the identities of applicants and ensure the confidentiality of the investigations; and
- (i) implement all interceptions in such a manner that neither the interception target nor another applicant is aware of any changes made to fulfil the warrant.

(2) A service provider who fails to give assistance in terms of this section commits an offence and is liable to a fine not exceeding P50 000 and each director also commits an offence and is liable to imprisonment for a period not exceeding 10 years unless the director establishes that he or she took reasonable precautions and exercised due diligence to avoid the commission of the offence.

(3) The Authority may revoke the licence of a services provider or protected information key holder who discloses information in contravention of subsection (1).

PART IV — *Handling of Information from Controlled Investigations* (ss 25-27)

Handling of
information

25. The head of an investigatory authority shall ensure that reasonable care is taken to protect and preserve information where evidence gathered from a controlled investigation is sufficient for analysis in a controlled investigation.

Retention and
storage of
information

26. (1) The head of an investigatory authority shall retain information obtained through controlled investigations as may be prescribed.

(2) The court may, on application by an applicant, order that information obtained from the carrying out of a controlled investigation in respect of a serious crime related activity shall be retained, if the court is satisfied that there are reasonable grounds to believe that —

- (a) the information obtained from the analysis of the controlled investigation is likely to produce evidence of probative value in relation to an offence; and
- (b) during the controlled investigation there may be information that may lead to a conviction.

(3) A court order granted under this section shall state the period for which the information obtained may be retained.

27. (1) A recording made on audiotape, videotape other electronic or other means by an applicant acting in terms of this Act, that is not required for investigative or evidentiary purposes, may be retained for such purpose and period as the Minister may direct.

Retention of electronic record

(2) The Minister shall prescribe the manner and time frame for the retention of the matter referred to in subsection (1).

PART V — *Admissibility of Evidence (ss 28-31)*

28. (1) Any evidence obtained through a controlled investigation carried out in accordance with this Act shall be admissible as evidence in court.

Legally obtained information

(2) The court may consider the following, in deciding whether to admit the evidence referred to in subsection (1), —

- (a) the probative value of the evidence, including whether evidence of equivalent probative value could have been obtained by other means; and
- (b) all relevant factors which, in the opinion of the court, are necessary for arriving at such a decision.

29. Any evidence relating to the details as to how a controlled investigation was carried out shall be admissible in court —

Evidence relating to carrying out of controlled investigation

- (a) to establish or rebut an allegation that unreasonable force was used during the carrying out of the controlled investigations; or
- (b) to decide the admissibility of a confession or admission, or other evidence averse to the suspect if the suspect alleges that the evidence was induced or obtained by the use of unreasonable force.

30. Information contained in a communication retained in a foreign State in accordance with the law of that foreign State and certified by a judicial officer of that foreign State to have been so intercepted and retained, shall be admissible as evidence in proceedings for an offence under this Act.

Admissibility of evidence from foreign State

31. Any evidence not obtained in terms this Part, shall not be admissible as evidence in court.

Inadmissible evidence

PART VI — *Miscellaneous Provisions (ss 32-34)*

32. An action shall not be brought against any member of staff of an investigatory authority or any other officer (or any other person authorised by the court to perform any act under this Act), in respect of anything done while taking part in the authorised conduct granted in terms of this Act.

Legal indemnity

33. (1) A person who delays, interferes with or wilfully obstructs an applicant in the exercise of the powers conferred under this Act, commits an offence and is liable to a fine not exceeding P10 000 or to a term of imprisonment for a period not exceeding 12 years, or to both.

Offences and penalties

B.16

(2) A person who contravenes an authorisation or warrant issued under this Act commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding 15 years, or to both.

Regulations

34. (1) The Minister may make regulations prescribing anything under this Act which is to be prescribed, or which is necessary or convenient to be prescribed, for the better carrying out of the objects and purposes of this Act.

(2) Without prejudice to the generality of subsection (1), regulations may provide for —

- (a) reporting obligations of an investigatory authority;
- (b) measures to ensure the security of information disclosed by or to the investigatory authority; and
- (c) the manner and form an investigatory authority is to keep records required under this Act.