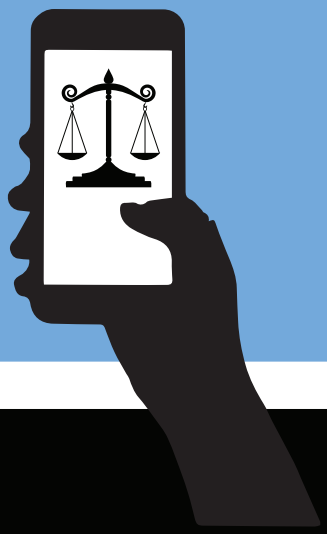
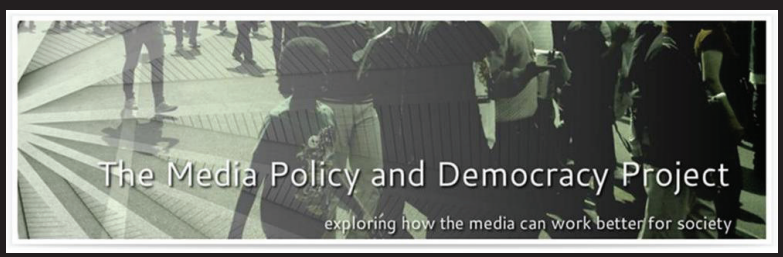
Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework



Tachilisa Badala Balule

November 2021



Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework

A report compiled by

Tachilisa Badala Balule

Tachilisa Balule is an Associate Professor of Law in the Department of Law, University of Botswana. He is currently the Deputy Dean in the Faculty of Social Sciences. He holds an LLB degree from the University of Botswana, and LLM and PhD degrees from the University of Edinburgh, Scotland. His PhD research was on regulation of the media. Dr Balule has published in the area of freedom of expression, including media freedom and access to information, and on aspects of electoral laws. He has delivered a number of papers on freedom of expression, media law and access to information at national and international conferences.

This report was commissioned by the Media Policy and Democracy Project (MPDP) supported by a grant from Luminate. The MPDP is a joint project of the University of Johannesburg's Department of Communication and Media and the University of South Africa's Department of Communication Science.

November 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

Table of Contents

Introduction

Surveillance of digital communications content data can be a necessary and effective tool for legitimate law enforcement or intelligence purposes. It may be done to conduct surveillance and interception of private communications in order to gather information that is necessary to prevent attempts to commit serious crimes or to identify perpetrators for the purpose of holding them accountable through the criminal justice system.[1] Surveillance of communications may target a particular individual or individuals or an organisation or group, or it may be done in bulk. The latter is a method of strategically monitoring transnational signals in order to screen them for certain cue words or key phrases.[2] Bulk interception of communications is generally used for the purpose of foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism.[3] The use of surveillance technologies results in a prima facie violation of an individual's right to privacy. This is because, surveillance interferes with the integrity and confidentiality of an individual's correspondence, and the collection and retention of communications data may interfere with privacy. In the digital age, many people are now using internet-based communications technologies and mobile smartphones, among others, to communicate. The flipside of this development is that the use of communications technologies has also enhanced the capacity of governments to conduct surveillance in the form of interception of communications and data collection on individuals. It has been observed that overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure.[4] Examples of overt digital surveillance may take the form of closed-circuit television monitoring while covert will include surveillance of individual's communications without their knowledge. The UN High Commissioner for Human Rights has noted with concern that, in many countries around the world, surveillance is used to target specific individuals such as opposition figures, critics of the government and journalists.[5]

Surveillance of digital communications by law enforcement agents, especially in environments where it is unlawful, not only infringes upon the right to privacy, but other fundamental rights too. The knowledge or suspicion of surveillance will restrict individuals' capacity to exercise their rights to freedom of expression, association and religious beliefs.[6] Weak regulatory environments provide fertile ground for arbitrary and unlawful communications surveillance by States. The UN High Commissioner for Human Rights has raised concern over the lack of adequate national legislation, procedural safeguards and effective oversight, which all contribute to a lack of accountability for unlawful digital surveillance. These concerns culminated in the UN General Assembly adopting Resolution 68/167, which calls upon Member States to ensure that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework which is publicly accessible, clear, precise, comprehensive and non-discriminatory.[7]

1 J A Mavedzenge, 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantee Proportionality in Communications Surveillance' 2020 (2) *African Journal of Legal Studies* 360, 361.

2 *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, CCT 278/19 (Constitutional Court, unreported delivered on 04 February 2021) para 4.

3 *Big Brother Watch and Others v United Kingdom,* Application nos. 58170/13 and 24960/15 (ECtHR, unreported, 25 May 2021) para 345.

4 UN Human Rights Council, *The right to privacy in the digital age* (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/27/37, 2014) para 2.

5 Ibid, para 3.

6 UN Human Rights Council, *Surveillance and human rights* (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, 2014) para 21.

7 UN General Assembly, *The right to privacy in the digital age* (Resolution adopted by the General Assembly, A/RES/68/167, 2014) para 4.

There are several law enforcement agencies in Botswana whose mandate may require them to resort to surveillance of digital communications in the performance of their respective roles. These agencies include the Botswana Police Service, the Directorate on Corruption and Economic Crime (DCEC), and the Directorate of Intelligence and Security (DIS). The critical question that arises is whether the State of Botswana has in place a domestic legal framework regulating surveillance of digital communications which meets the standards required by international human rights law. There have been persistent concerns in Botswana that law enforcement agencies are using surveillance of digital communications in an arbitrary and unlawful way to target specific individuals.[8] In 2014, it was reported in a local newspaper that the DIS was being used by the State to monitor activities of opposition members, critics of the government and human rights activists. Another newspaper reported that the DIS had engaged an Israeli company to supply it with a spyware that has capability to spy on emails, Facebook and Twitter.[9] Yet another newspaper reported that the DIS is one of the few intelligence agencies in the world using the Israeli hackers' Circle Spyware.[10] It is alleged that the software exploits weaknesses in the global mobile phone systems to snoop on calls, texts, and the location of phones around the globe. Members of the opposition have over the years expressed concern over the DIS being used by the State to unlawfully monitor their activities. Local media has also reported that the Botswana Police Service has acquired a Universal Forensic Extraction Device (UFED), sold by an Israel-based company, Cellebrite, and a Forensic Toolkit (FTK), from a US-based company, Access Data. The two technologies are said to have capabilities for extracting information from phones and computers, and breaking into locked devices and decrypting information.[11] The concerns that law enforcement agencies are using surveillance measures in an arbitrary and unlawful way are difficult to verify. There are no mechanisms in place to compel the agencies to disclose whether an individual was a subject of surveillance measures. The apprehension that law enforcement agencies are using surveillance measures unlawfully and arbitrarily cannot be lightly dismissed. The mere existence of a secret regime of monitoring constitutes an interference with the right to privacy.[12] This calls for sufficient and effective measures to be put in place to protect the right to privacy.

The research paper critically assesses the legal framework regulating the surveillance of digital communications by law enforcement agencies in Botswana. The aim is to determine whether the legal framework meets the standards required by international human rights law for the protection of the right to privacy. The paper focuses on surveillance measures that enable an actor to gain surreptitious access to digital communications, browsing data, location history and online and offline activities of individuals. The research paper is divided into two key parts. Part one provides an overview of the protection of the right to privacy. It examines the relevant constitutional provisions and international human rights treaties on protection of the right to privacy in Botswana. In part two, the paper looks at the legislative framework that permits surveillance of individuals' digital communications in Botswana. It also critically assesses the legal framework to determine whether it meets the standards required by the Constitution and international human rights law for the protection of the right to privacy.

8 Online editor, 'Kapinga moves to stop "criminal behaviour" of tapping phones' *Sunday Standard* (Gaborone, 10 November 2016). <www.sundaystandard.inform> accessed 14 July 202;1 and 'DIS launches massive surveillance programme' *Botswana Guardian* (Gaborone, 25 February 2015. < www.botswanaguardian.co.bw> accessed 14 July 2021.

9 Ibid.

10 Letlhogile Mpuang, 'The Spies Are Listening: How DISS Bugs Your Phones – US Report' *Botswana Gazette* (24 March 2021) 3.

11 Jonathan Rozen, 'Equipped by US, Israeli firms, police in Botswana search phones for sources' (*Committee to Protect Journalists*, 5 May 2021. < https://cpj.org/2021/05/equipped-us-israeli-firms-botswana-police>.

12 *Szabo and Vissy v Hungary*, Application no. 37138/14 (ECtHR, unreported, 12 January 2016) para 53.

Protection of the right to privacy in Botswana

The right to privacy is accorded constitutional protection in the following terms:

(a) Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises.

(b) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision –

(i) that is reasonably required in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development and utilisation of mineral resources, for the purpose of any census or in order to secure the development or utilisation of any property for a purpose beneficial to the community;

(ii) that is reasonably required for the purpose of protecting the rights or freedoms of other persons;

(iii) that authorises an officer or agent of the Government of Botswana, a local government authority or a body corporate established by law for a public purpose to enter on the premises of any person in order to inspect those premises or anything thereon for the purpose of any tax, rate or duty or in order to carry out work connected with any property that is lawfully on those premises and that belongs to that Government, authority or body corporate, as the case may be; or

(iv) that authorises, for the purpose of enforcing the judgment or order of a court in any civil proceedings, the search of any person or property by order of a court or entry upon any premises by such order, and except so far as that provision or, as the case may be, anything done under the authority thereof is shown not to be reasonably justifiable in a democratic society.[13]

The High Court of Botswana has observed that the right to privacy is multifaceted and multipronged, and thus defies precise definition.[14] The court further noted that privacy is context based and must be interpreted in the light of the current era and context.[15] The right to privacy, arguably, has two facets, namely substantive and informational autonomy.[16] Substantive privacy is the presumption that a person should have a private sphere with or without interaction with others, free from unsolicited intervention by other uninvited individuals to make choices about personal life.[17] Informational autonomy on the other hand relates to an individual's interest in controlling the flow of personal information about them and how it is used.[18] Surveillance of an individual's digital communications data is an egregious invasion of the right to privacy. In this regard, the South African Constitutional Court has said that: '[By] nature, human beings are wont – in their private communications – to share their innermost hearts' desires or personal confidences, to speak or write

13 Section 9, Constitution of Botswana [Cap. 01].

14 Per Leburu J, in *Motshidiemang v Attorney General and Another*, MAHGB-000591-16 (High Court, unreported, 11 June 2019) para 114.

15 Ibid, paras 107 and 112.

16 H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (Oxford University Press 2006) 662.

17 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (A/HRC/23/40, 2013) para 22.

18 H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (n 16) 663.

when under different circumstances they would never dare do so, to bare themselves on what they truly think or believe. And they do all this in the belief that only hearers of what they are saying or the only readers of what they have written are those they are communicating with'.[19] Interception of an individual's communications data is indiscriminate and would include the most private and intimate, which has nothing to do with the reason for the surveillance.

A cursory look at section 9 (1) of the Constitution suggests that the provision guarantees only a limited right to privacy as it refers to protection against the search of his or her person, property, or entry by others on his or her premises. However, the High Court has held that the provision should be given a broad, generous and purposive interpretation.[20] A generous construction of a constitutional provision means that when interpreting a provision, courts should not whittle down any rights and freedoms unless by very clear and unambiguous words, such interpretation is compelling.[21] It also requires that when interpreting the provisions of the Constitution guaranteeing rights, a court must breathe life into the Constitution by having regard to its liberal values, and where necessary, use international human rights treaties that Botswana has subscribed to as an aid to interpretation.[22] Botswana has ratified the International Covenant on Civil and Political Rights (ICCPR) which guarantees the right to privacy, but has not domesticated it. International treaties do not confer enforceable rights on persons in Botswana until Parliament has legislated their relevant provisions into the law of the land.[23] The Court of Appeal has, however, ruled that as a member of the community of civilised States which have undertaken to abide by certain standards of conduct, unless it is impossible to do otherwise, it would be wrong for the courts to interpret legislation in a manner which conflicts with the international obligations Botswana has undertaken.[24] The Vienna Convention on the Law of Treaties provides that every treaty in force is binding upon the parties to it and must be performed in good faith.[25] Thus, when a State has ratified an international treaty, the judiciary, as part of the State, is also bound by such treaty.[26] Judges are therefore under an obligation to see that all the effects of the provisions embodied in a treaty are not adversely affected by the enforcement of laws which are contrary to its purpose.[27] The jurisprudence developed under the ICCPR on the right to privacy, though not binding on a court in Botswana, would play an important role in guiding a court in applying a broad, generous and purposive approach to the interpretation of section 9 (1) of the Constitution to ensure that the right to privacy in the country is accorded protection that complies with international human rights standards.

The Court of Appeal has further held that when interpreting the provisions of the Constitution, respect must be paid to the language which has been used and to the traditions and usages which have given meaning to that language.[28] The court proceeded to observe that the Bill of Rights in the Constitution of Botswana was influenced by the European Convention on Human Rights (ECHR), which was in turn influenced by the Universal Declaration of Human Rights (UDHR).[29] The Court of Appeal concluded that the antecedents of the Constitution of Botswana with regard to the imperatives of the international community

19 *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (n 2) para 23.

20 *Motshidiemang v Attorney General and Another* (n 12) para 116, and *Ketlhaotswe and Others v Debswana Diamond Company (Pty) Ltd*, CVHGB-001160-07 (High Court, unreported, 27 September 2022) para 34.

21 Per Aguda, J.A, in *Attorney General of Botswana v Dow* [1992] BLR (CA) 119, 165.

22 Ibid, 166 and *Ramantele v Mmusi and Others,* CACGB-104-12 (Court of Appeal, unreported, 3 September 2013) para 69.

23 *Attorney General of Botswana v Dow* (n 21) 154, and *Good v The Attorney General* [2005] 2 BLR 337.

24 Ibid.

25 Article 26.

26 *Case of Almonacid Arellano et al. v Chile.* Preliminary objections, merits, reparation and costs. (Inter-American Court of Human Rights, judgment of September 26, 2006) Series C No. 124, para 19.

27 Ibid.

28 *Attorney General of Botswana v Dow* (n 21) 152.

29 Ibid.

call for a generous interpretation of the provisions of the Constitution to give to individuals the full measure of their fundamental rights and freedoms.[30] A broad, generous and purposive interpretation of the provisions in the Bill of Rights that would give individuals a full measure of the rights and freedoms guaranteed to them would thus permit a court to seek guidance from the jurisprudence that has been developed under both the UDHR and ECHR on a similar right or freedom. It has been argued that a broad, generous and purposive interpretation of the provisions of the Constitution demands that when interpreting a provision, it is not just possible, but imperative that judges investigate how similar issues have been resolved in other jurisdictions due to the fact that many constitutions around the world have been inspired by the same philosophy.[31] It is submitted that the relevant provisions of the UDHR and ECHR on the right to privacy and the jurisprudence developed thereon, though not binding on a court in Botswana, would be highly persuasive in the interpretation of section 9 (1) of the Constitution because the provision was inspired by the liberal values espoused in these human rights instruments.[32] The writer contends that even though section 9 (1) may appear to be guaranteeing a limited right to privacy, a broad, generous and purposive interpretation of the provision will embrace both substantive privacy and informational autonomy.

The guarantee of a right such as privacy under the Constitution imposes both negative and positive obligations on the State.[33] The negative obligation obligates the State to avoid interfering with the right to privacy unless the conditions for justifying the interference are satisfied.[34] The positive obligation, on the other hand, requires the State to take positive steps to protect the right to privacy, especially against interference by others.[35] Surveillance of individuals' digital communications by law enforcement agencies raises the issue of the State's negative obligation not to interfere with the right to privacy unless the conditions for interference are satisfied.

The right to privacy guaranteed under the Constitution is not absolute. Interference with the right is permissible under section 9 (2), provided such interference complies with the conditions set therein. The provision lays down a stringent three-part test which any interference with the right must comply with for it to be legitimate.[36] The test requires that an interference with the right to privacy must comply with all of the following conditions:

(a) It must be contained in or done under the authority of the law;
(b) The interference must be shown to be for the purpose of protecting any of the interests listed in the provision;
(c) And it must be shown to be reasonably justifiable in a democratic society.

The requirements of the above test are intended to ensure that any derogations from the right to privacy are given a strict and narrow construction. The courts of law in Botswana have not yet had occasion to elaborate on what each of the three components of the test entail. Although the provision may appear to be broadly framed, courts have shown that they will adopt a narrow a strict approach when dealing with limitations.[37] Guidance on what the test entails must be sought from international human rights law and foreign comparative law as a way of according the provision a broad, generous and purposive interpretation. Such an approach demands that judges in Botswana should investigate how similar issues have been resolved in other jurisdictions. Both the ICCPR

30 Ibid.
31 CM Fombad, 'Enhancing the Judicial Role in Human Rights Protection in Botswana' in E Quansah and W Binchy, *The Judicial Protection of Human Rights in Botswana* (Clarus Press, 2009) 133 at 150.
32 See *Petrus and Another v State* [1984] BLR 14 (CA).
33 UN Human Rights Committee, General Comment No. 31: The Nature of the General Obligations Imposed on States Parties to the Covenant, (CCPR/C/21/Rev.1/Add.13, 2004) [6].
34 Ibid.
35 Ibid.
36 *Motshidiemang v Attorney General and Another* (n 14) para 119.
37 Ibid, para 119.

and ECHR have similar tests on limitations on the right to privacy. The ECHR provides that for an interference with the right to privacy to be lawful, it must meet the following three conditions: (i) it must be in accordance with the law; (ii) pursue one of the several legitimate aims identified under Article 8(2); and (iii) be necessary in a democratic society.[38] Article 17 of the ICCPR, which guarantees the right to privacy, does not contain a limitation clause. Despite the absence of a limitation clause, it is generally understood that the guarantee of the right to privacy should be interpreted as containing elements of a permissible limitations test similar to the other rights and freedoms guaranteed in the ICCPR such as freedom of expression (Article 19 (3)); freedom to manifest one's religion or beliefs (Article 18 (3)); and the right of peaceful assembly (Article 21).[39] The limitation clauses in these Articles set forth three conditions that a limitation on the guaranteed rights must conform to. The conditions are that the limitation must be provided by law, serve a legitimate interest, and be reasonably justifiable in a democracy. The Human Rights Committee (HRC) and European Court of Human Rights (ECtHR) have developed extensive jurisprudence on the requirements of the limitation tests in the respective treaties which can be used as a guide in the interpretation of the right to privacy under the Constitution of Botswana.

The first part of the constitutionality test is that the interference must be 'contained in or done under the authority of the law'. The wording used in the ICCPR is that any interference with the right to privacy must be 'provided by law' while the ECtHR uses the phrase 'in accordance with the law'. When interpreting a similarly worded provision in the 1980 Zimbabwean Constitution, the Zimbabwean Supreme Court held that, although worded differently from the phrases used in international human rights treaties such as the ICCPR and ECtHR, the phrase 'contained in or done under the authority of the law' carries essentially the same meaning.[40] When elaborating on the meaning of the phrase 'in accordance with the law', the ECHR as held that it has two aspects. First, that the impugned measure should have some basis in the domestic law.[41] And secondly, the law must be accessible to the person concerned and foreseeable as to its effects.[42] The second aspect requires that the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances under which public authorities are empowered to resort to surveillance measures.[43] The ECtHR has, however, said foreseeability in the context of interception of communications cannot be the same as in many other fields.[44] The court explained that foreseeability in the special context of secret measures of surveillance of communications does not mean that an individual should be able to foresee when authorities are likely to resort to such measures so that they can adapt their conduct accordingly.[45] But the law must be sufficiently clear to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to surveillance measures.[46]

The ECtHR has further held that the second aspect of 'in accordance with the law' is also about the quality of the law. A law authorising secret surveillance must provide adequate and effective safeguards and guarantees against abuse.[47] The court recognises that where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. Consequently, the ECtHR has developed in its case-law on interception of communications, minimum requirements that

38 Article 8 (2) ECHR.

39 See UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (n 17) para 29.

40 *Chavunduka and Another v Minister of Home Affairs 2000* (1) ZLR 552 at 560.

41 *Szabo and Vissy v Hungary* (n12) para 59.

42 *Big Brother Watch and Others v United Kingdom* (n 3) para 332.

43 *Liberty and Others v United Kingdom,* Application no. 58243/00 (ECtHR, unreported, 01 July 2008) para 59.

44 *Szabo and Vissy v Hungary* (n 12) para 62.

45 *Big Brother Watch and Others v United Kingdom* (n 3) para 333.

46 Ibid.

47 *Szabo and Vissy v Hungary* (n 12) para 59.

should be set out in law in order to avoid abuses of power.[48] The requirements are that the law must clearly spell out:

(a) The nature of offences which may give rise to an interception order;
(b) A definition of the categories of people liable to have their communications intercepted;
(c) A limit on the duration of interception;
(d) The procedure to be followed for examining, using and storing the data obtained;
(e) The precautions to be taken when communicating the data to other parties; and
(f) The circumstances in which intercepted data may or must be erased or destroyed.[49]

The ECtHR has clarified that the first two of the six safeguards above are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence.[50] Nevertheless, the court considers it imperative that when a State is operating a bulk surveillance regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, the domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted.[51]

The second limb of the constitutionality test interrogates whether the interference pursues any of the several legitimate aims stated in section 9 (2) of the Constitution. Many states the world over are faced with the challenges of terrorism and organised crime. These activities threaten to destroy states and societies, thus, a state may justify interception of digital communications for the purpose of protecting national security or public order. These two are recognised legitimate interests that may justify interference with the right to privacy under the Constitution of Botswana. Botswana, like many countries around the world, is faced with threats of terrorism. In addition, it also faces challenges of organised crime, especially poaching in game reserves, which is threatening endangered species such as rhinos. Law enforcement agencies generally find this limb of the test easy to satisfy in light of the broad terms in which the legitimate purposes are framed.

The third part of the constitutionality test is that an interference with the right to privacy must be reasonably justifiable in a democracy. The ECtHR has opined that this requires a state which is seeking to interfere with the right to privacy to establish two things. First that the impugned measure in question is responding to a pressing social need.[52] The inquiry here is not whether surveillance is desirable or convenient, but whether, given the circumstances of the case, there is a pressing need to conduct surveillance in order to protect a legitimate interest.[53] Secondly, the interference should be no greater than is necessary to address the pressing social need. This means that the terms and conditions of surveillance should be proportionate in the sense that they should not subject the targeted person to surveillance whose nature, extent, and scope is more than what is necessary to achieve the purpose for which the surveillance was authorised.[54]

48 *Big Brother Watch and Others v United Kingdom* (n 3) para 335.
49 Ibid.
50 Ibid, para 348.
51 Ibid.
52 *Silver v United Kingdom* (1983) 5 EHRR 737, para 48.
53 J A Mavedzenge, 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantee Proportionality in Communications Surveillance', (n 1) at 365.
54 Ibid.

The ECtHR has held that where a law permitting secret surveillance is contested before a court of law, the first limb of the test is closely related to the third limb and should be addressed jointly.[55] The court elaborated in this regard that the quality of the law implies that the domestic law must not only be accessible and foreseeable in its application, but must also ensure that secret surveillance measures are applied only when necessary in a democratic society, in particular, by providing for adequate and effective safeguards and guarantees against abuse.[56] An assessment of the necessity of measures will thus require a court to examine the safeguards of foreseeability, and in addition, have regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by the law.[57] With regard to bulk interception, the ECtHR has held that in order to minimise the risk of the power being abused, the process must be subject to end-to-end safeguards.[58] This will require that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined, and that the operation should be subject to supervision and independent *ex post facto* review.[59]

55 *Big Brother Watch and Others v United Kingdom* (n 3) para 334.
56 Ibid.
57 Ibid, para 335.
58 Ibid, para 349.
59 Ibid, para 350.

Legislative framework on surveillance of communications in Botswana

Botswana does not have a general statute, like some countries such as South Africa, which regulates interception of individuals' communications by law enforcement agencies in the performance of their respective mandates. However, there are currently two provisions in two different statutes that permit specified judicial officers to grant communications interception orders for law enforcement purposes. One provision is found in the Counter-Terrorism Act.[60] This Act provides for, among others, measures to prevent and combat terrorism, including financing of terrorism. Section 20 of the Act reads:

(a) Subject to subsection (2), an investigating officer may, for the purpose of obtaining evidence of the commission of an offence under this Act, apply *ex parte* to a magistrate court or the High Court, for an order to intercept communications.

(b) A magistrate or judge to whom an application is made under subsection (1), if satisfied that there are reasonable grounds to believe that material information relating to –

(i) the commission of an offence under this Act; or

(ii) the whereabouts of a person suspected to have committed an offence, is contained in the communication, may make an order –

- requiring a communication service provider to intercept and retain specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communication service provider,
- authorising an investigation officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication or other communication of a specified description, and to remove and retain such device, or
- authorising an investigation officer to use any other method of interception.

(iii) An order made in subsection (2) shall be for a period not exceeding 90 days in first instance and may, on application made by the investigating officer, be extended for a further period, provided that a judge is satisfied that grounds of suspicion still exist, and the maximum period of extension does not exceed 180 days.

The above provision permits a Magistrate's Court or High Court to issue an order to intercept communications for purposes of obtaining evidence of the commission of an offence under the Act. The offences for which an interception order can be issued under the provision include an act of terrorism, offences associated with or connected to acts of terrorism, and financing terrorism.[61] An application for an interception order must be made by an investigating officer who can be a member of the Botswana Police Service, Botswana Defence Force or DIS. The Act excludes members of the DCEC. The provision will apply to cases of targeted surveillance where a person is being investigated for commission of an offence under the Act.

60 Act 24 of 2014 [Cap. 08:08], Laws of Botswana.

61 See Part II of the Counter-Terrorism Act.

The Intelligence and Security Services Act, 2007 (ISSA)[62] also has a provision under which a communications interception order may be obtained. Section 22 in the relevant parts states:

(a) Where the Director General believes, on reasonable grounds, that a warrant under this section is required to enable the Directorate to investigate any threat to national security or to perform any of its functions under this Act, the Director General shall apply to a senior magistrate or judge of the High Court for a warrant in accordance with this section…

(d) The court mentioned in subsection (1) may, on application made by the Director General or an officer or support staff authorised by him or her to do so, issue a warrant under this section authorising the taking of such action as may be specified in the warrant in respect of anything so specified if the court considers it necessary for that action to be taken in order to obtain information which –
   (a) is likely to be of substantial value to the Directorate in the discharge of its functions; and
   (b) cannot be reasonably obtained through other means:

Provided that in the event the Directorate wishes to conduct an investigation of a personal or intrusive nature such as searches or interception of postal mail, electronic mail, computer or telephonic communications, the Director General or an officer or support staff authorised by him or her shall show cause to a court of Senior Magistrate or above or a Judge of the High Court and obtain an order in a secret hearing.

The functions of the DIS include the detection and identification of threats and potential threats to national security and 'other duties and functions as from time to time be determined by the President to be in the national interest'.[63] Section 22 allows the Director General of the DIS to apply to a Senior Magistrate or Judge of the High Court for a warrant to intercept communications where she/he believes, on reasonable grounds, that the information obtained is likely to be of substantial value in the discharge of the DIS's functions. The provision can be used to obtain orders for both targeted and bulk interception.

The sections in the Counter-Terrorism Act and ISSA are the only ones that permit courts of law in Botswana to issue communications interception orders for law enforcement purposes. Any interception not based on the two provisions will thus not have any basis in law and is therefore unconstitutional. The critical question is whether the two provisions that permit interception of communications meet the threshold required by section 9 (2) of the Constitution. A determination of this question requires that the provisions be assessed against the constitutionality test. Due to the unavailability of local case-law on the subject, the discussion will borrow from international human rights law jurisprudence. This approach is in line with the principle that has been laid down by the courts of law in the country that, when interpreting the provisions of the Constitution, a broad, generous and purposive approach should be adopted. This will entail, among others, that when interpreting a provision in the Constitution, it is important to investigate how similar issues have been resolved in other jurisdictions. It must be noted that the absence of case-law on the application of the two provisions does not mean the provisions are not used or are rarely used. There is so much secrecy in the application of the provisions such that those who are targeted never get to know and are thus deprived the opportunity to seek redress in the courts.

The first limb of the constitutionality test, 'done under the authority of the law', has two facets. The interception measures should have some basis in the domestic law and the law must be accessible and foreseeable as to its effects. An interception of communications pursuant to any of the two

62 Act No. 16 of 2007, Laws of Botswana.

63 Ibid, section 5 (1).

provisions would satisfy the first facet of this limb of the constitutionality test. It is the second facet that raises some questions. A law that interferes with the right to privacy must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances under which public authorities are empowered to interfere with the right. The Counter-Terrorism Act allows for a communications interception order for the purpose of obtaining evidence of the commission of an offence under the Act. The offences for which an interception order can be granted by the courts are stipulated in Part of the Act. It is thus contended that the provision is sufficiently clear in its terms to give individuals an adequate indication on the circumstances under which law enforcement agencies may be granted a communications interception order under the Act.

The provision in the ISSA, on the other hand, raises questions relating to the element of foreseeability. The DIS is mandated with the responsibility of detecting and identifying threats and potential threats to national security. In addition, it also performs other duties and functions as from time to time be determined by the President to be in the national interest. It is argued that what will constitute a threat or potential threat to national security is not sufficiently clear to give individuals an adequate indication on the circumstances under which the DIS may be empowered to intercept their communications. The Act defines threats to national security as:

(a) Any activity relating to espionage, sabotage, terrorism or subversion, or intention to engage in any such activity directed against, or detrimental to the interest of Botswana and includes any other activity performed in conjunction with any activity relating to espionage, sabotage, terrorism or subversion, but does not include any lawful advocacy, protest or dissent not performed in conjunction with any such activity;

(b) Any activity directed at undermining, or directed at or intended to bring about the destruction or overthrow of, the constitutionally established system of government of Botswana by unlawful means;

(c) Any threat or act of violence or unlawful harm directed at or intended to achieve, bring about or promote any constitutional, political, industrial, social or economic objective or change in Botswana and includes any conspiracy, incitement or attempt to commit any such act or threat; and

(d) Any foreign-influenced activity within or related to Botswana that –
   (i) is detrimental to the interest of Botswana, and
   (ii) is clandestine or deceptive or involves any threat to the State or its citizens or any person lawfully resident in Botswana.[64]

The concept of national security is an elusive one that defies precise definition in law because threats to national security vary in character and may be difficult to anticipate in advance. Despite the difficulties in conclusively defining threats to national security, international law offers guidance on what would constitute genuine threats to national security. The position under international law is that national security should be about protecting a country's political independence or territorial integrity from the use, or threatened use of force.[65] It is submitted that paragraphs (a) to (c) are clear on what activities will constitute threats to national security. The activities covered in these provisions relate to those that will undermine Botswana's political independence or territorial integrity through the use or threatened use of force.

64 Ibid, section 2.

65 See Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc. E/CN.4/1985/4, Annex no. 30 (1985), principle 29 and *Johannesburg Principles: National Security, Freedom of Expression and Access to Information* (adopted on 1 October 1995), principle 2.

It is contended that paragraph (d) above fails the foreseeability requirement. In defining threats to national security, the clause refers to 'any foreign-influenced activity'. There is no qualification that such activity should relate to the acts identified in the preceding paragraphs. The provision is widely crafted and would include activities that pose no threat to the security of Botswana. The provision further states that the activity must be 'detrimental to the interest of Botswana'. This phrase is borrowed from laws enacted in the United Kingdom such as the Official Secrets Act, 1911 which used the phrase 'interest of the State'. When interpreting this phrase, the House of Lords held that the phrase is identical with whatever the government of the day lays down as public policy.[66] It is contended that the meaning of the phrase 'interest of Botswana' is similar to 'interest of the State'. The Zimbabwean Supreme Court, when interpreting the meaning of the phrase 'interest of Zimbabwe', concluded that 'interest of the State' and 'interest of Zimbabwe' are the same. The court observed that if the provisions of a statute sought to be construed have nothing to do with the common law, the interpretation rendered to similar provisions in a foreign statute cannot be justifiably ignored.[67] The executive is given unfettered discretion under the ISSA to decide what is in the interest of Botswana, and the danger is that the discretion can be easily abused. There is no objective criteria that individuals can gauge what acts will be considered to be detrimental to the interest of Botswana. The clause also provides that the foreign-influenced activity must involve 'any threat to the State or its citizens'. The expression 'any threat' is too wide and can be construed by the executive to include acts that do not pose any threats to the country's political independence or territorial integrity against the use or threat of force, but that may be merely inconvenient or embarrassing to the executive. Paragraph (d) is not formulated with sufficient precision to give individuals an adequate indication on the circumstances under which the DIS may be empowered to intercept their communications.

One other concern with the ISSA is that the President is given wide discretion to assign additional duties to the DIS. The Act does not give the scope of the President's discretion in this regard or the manner of its exercise. There is no indication of what these duties and functions are. The effect of this on the right to privacy is that the President may exercise the discretion in a way that may require the DIS to monitor individual's communications. The discretion given to the President under the Act therefore does not give individuals adequate indication as to the circumstances under which the DIS may be empowered to interfere with the right to privacy.

In addition to foreseeability, the second facet of the constitutionality test also deals with the quality of the law. A law on surveillance of communications must provide adequate and effective safeguards and guarantees against abuse. The minimum standards developed by the ECtHR will be applied to the legal framework regulating interception of communications in Botswana to assess whether it provides adequate and effective safeguards against abuse. A determination of this issue is linked to the third limb of the constitutionality test as it will also address the question whether the surveillance measures are necessary in a democratic society.

(a) **Is the nature of offences clearly spelt out?**
The Counter-Terrorism Act lists all the offences which may give rise to an interception order. The ISSA on the other hand does not provide all the offences that could lead to an interception.

(b) **Categories of people liable to have communications intercepted.**
Since the Counter-Terrorism Act lists all the offences which may give rise to an interception order, it is argued that, by extension, this also gives a definition of categories of people liable to have their communications intercepted. Any person

66 *Chandler v D.P.P* [1962] 3 ALL E.R. 142. See the speeches of Lord Devlin and Lord Pearce at 156 and 160, respectively.

67 *S v Harrington* 1989 2 SA 348.

who is involved or suspected to be involved in the commission of the stated offences may be a target of an interception order. The ISSA fails to define categories of persons whose communications may be intercepted. This is due to the failure of the Act to conclusively define threats to national security and the powers given to the President to assign the DIS additional powers could also lead to interception of communications.

(c) **Limit on duration of interception.**
The ISSA does not prescribe any time limit on the duration of an interception order. The Counter-Terrorism Act prescribes that an initial interception order shall be for a period not exceeding ninety days and can be extended for a period not exceeding one hundred and eighty days.

(d) **Procedure for examining, using and storage of data.**
Neither the ISSA or Counter-Terrorism Act have provisions relating to the management of intercepted data. Only the former provides for the destruction of irrelevant data, but does not say anything about the management of retained information.[68] The lack of regulation on the management of intercepted data may expose subjects to further intrusions into their right to privacy.

(e) **Communication of data to third parties.**
Neither Act addresses the precautions to be taken when communicating intercepted data to other parties.

(f) **Destruction of intercepted data.**
Save for the destruction of irrelevant data in the ISSA, the two Acts regulating issuance of communications interception orders do not say anything on the destruction of communications data.

The above assessment of the communications interception regime in Botswana reveals that it does not have in place adequate and effective safeguards and guarantees against abuse. The absence of these safeguards would make the regime fail the second part of the first limb of the constitutionality test relating to the quality of the law. The absence of adequate and effective safeguards against abuse also make the communications interception regime fail the third limb of the constitutionality test. Failure to provide for safeguards against abuse will subject the target of surveillance to an interference with the right to privacy whose nature, extent, and scope will be more than what is necessary to achieve the purpose for which the surveillance was authorised.

Another important safeguard against abuse of surveillance measures is the requirement of post-surveillance notification to the subject. The South African Constitutional Court has observed that the vast majority of subjects of surveillance never become aware of their surveillance and that this facilitates the abuse of the process.[69] The court concluded that post-surveillance notification is an absolutely necessary safeguard of the right to privacy because it will go a long way towards eradicating impunity. It is submitted that the absence of post-surveillance notification under both the ISSA and Counter-Terrorism Act will also render the interception regimes under the laws unconstitutional for failure to provide adequate and effective safeguards against abuse of surveillance measures by law enforcement agencies.

The interception of communications regime under the ISSA permits bulk interception. Bulk interception is used for foreign intelligence gathering, counter-espionage and counter-terrorism. The functions of the DIS include the detection and identification of threats and potential threats to national security. This will allow the DIS to apply for a bulk interception order. Although the legal framework under the ISSA permits

68 Section 44 (1), Intelligence and Security Service Act, 2007 (n 59).

69 *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (n 2) para 43.

bulk interception of communications, the exact capabilities of the DIS to conduct such are unknown and are only the subject of speculation. There are no mechanisms in place to compel the institution to disclose its capabilities to conduct bulk interception. It is however submitted that the bulk interception regime fails the second part of the first limb of the constitutionality test. In particular, the regime fails to provide adequate safeguards to guard against abuse. While the issuance of a bulk interception order is subject to independent authorisation, the operation is not subject to supervision and independent *ex post facto* review. Furthermore, the absence of these measures will make any bulk interception under the Act fail the third limb of the constitutionality test. An interception regime cannot be reasonably justifiable in a democracy where there are no adequate measures in place to guard against abuse.

The issue of the availability of sufficient and adequate safeguards also raises the important matter of judicial oversight of communications surveillance. Both the Counter-Terrorism Act and ISSA allow a magistrate or a judge of the High Court to issue an interception order. Interception of individuals' private communications for law enforcement purposes presents a situation of conflict between the individual's right to privacy and the public interest. The judiciary therefore, because of its independence from the executive, would be the appropriate organ to adjudicate on the dispute. The involvement of the judiciary is thus an important supervisory measure as a court of law will be better placed to carry out a balancing exercise between the competing interests of the individual and the state. While it is commendable that the interception regime provides for judicial oversight, it is argued that the involvement of magistrates in consideration of applications for interception is inappropriate. The Constitution of Botswana provides that in any proceedings before a subordinate court where any question as to the interpretation of the Constitution arises, and the court is of the opinion that the question involves a substantial question of law, the court may or shall, if requested by any party to the proceedings, refer the matter to the High Court.[70] It is submitted that an application for an interception order raises constitutional issues and a substantive question of law and further that, since the application will be ex parte, where the affected person would not have a chance to present arguments, it would be appropriate that applications should be heard by the High Court.

70 Section 105 (1), Constitution of Botswana (11).

Conclusion

The right to privacy in Botswana is guaranteed under the Constitution in a way that is consistent with the guarantee of the right under international human rights law. The right is not absolute and the Constitution contains a stringent test which any limitation on the right must comply with. Any law that purports to limit the right to privacy must comply with the standards emanating from the limitation clause. International human rights law has developed substantial jurisprudence elaborating on the standards on limitations on the right to privacy. Botswana has not developed case-law on the limitation clause on the right to privacy in the Constitution. The State of Botswana is under an obligation, however, to enact laws that are in compliance with its obligations under international treaties. Courts of law in the country are also under an obligation to interpret domestic laws in a manner which is consistent with the international obligations Botswana has undertaken.

It is disappointing that the State of Botswana does not have in place a comprehensive legal framework regulating the issue of interception of communications data for law enforcement purposes. It has been noted that a weak regulatory environment provides fertile ground for arbitrary and unlawful communications surveillance by the State. This appears to be the case with Botswana. This paper demonstrates that the existing legal framework is not adequate to guard against unlawful and arbitrary surveillance of communications for law enforcement purposes. What is even more disturbing is that any surveillance authorised by the courts under the existing laws will not even meet the requirements of the constitutionality test. The right to privacy in Botswana is not sufficiently and adequately protected against interference by law enforcement agents. Botswana must pay heed to the call by the UN General Assembly to enact a comprehensive law on communications interception that is in compliance with its international human rights obligations.

References

5.1 Case law

Almonacid Arellano et al. v Chile. Preliminary objections, merits, reparation and costs. (Inter-American Court of Human Rights, judgment of September 26, 2006) Series C No. 124.

Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others, CCT 278/19 (Constitutional Court, unreported delivered on 04 February 2021).

Attorney General of Botswana v Dow [1992] BLR (CA) 119.

Big Brother Watch and Others v United Kingdom, Applications nos. 58170/13 and 24960/15 (ECtHR, unreported, 25 May 2021).

Chandler v D.P.P [1962] 3 ALL E.R. 142.

Chavunduka and Another v Minister of Home Affairs 2000 (1) ZLR 552.

Good v The Attorney General [2005] 2 BLR 337.

Ketlhaotswe and Others v Debswana Diamond Company (Pty) Ltd, CVHGB-001160-07 (High Court, unreported, 27 September 2022).

Liberty and Others v United Kingdom, Application no. 58243/00 (ECtHR, unreported, 01 July 2008).

Motshidiemang v Attorney General and Another, MAHGB-000591-16 (High Court, unreported, 11 June 2019).

Petrus and Another v State [1984] BLR 14 (CA).

Ramantele v Mmusi and Others, CACGB-104-12 (Court of Appeal, unreported, 3 September 2013).

S v Harrington 1989 2 SA 348.

Silver v United Kingdom (1983) 5 EHRR 737.

*Szabo and Vissy v Hungary***,** Application no. 37138/14 (ECtHR, unreported, 12 January 2016).

5.2 Other Sources

Fenwick, H. and Phillipson, G. *Media Freedom under the Human Rights Act* (Oxford University Press, 2006).

Fombad, C.M. 'Enhancing the Judicial Role in Human Rights Protection in Botswana' in E. Quansah and W. Binchy, *The Judicial Protection of Human Rights in Botswana* (Clarus Press, 2009) 133.

Johannesburg Principles: National Security, Freedom of Expression and Access to Information (adopted on 1 October 1995).

Mavedzenge, J.A. 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantee Proportionality in Communications Surveillance' 2020 (2) *African Journal of Legal Studies* 360, 361.

Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc. E/CN.4/1985/4, Annex no. 30 (1985).

UN Human Rights Council, *The right to privacy in the digital age* (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/27/37, 2014).

UN Human Rights Council, *Surveillance and human rights* (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, 2014).

UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, (A/HRC/23/40, 2013) para 22.

UN Human Rights Committee, *General Comment No. 31: The Nature of the General Obligations Imposed on States Parties to the Covenant,* (CCPR/C/21/Rev.1/Add.13, 2004).

UN General Assembly, *The right to privacy in the digital age* (Resolution adopted by the General Assembly, A/RES/68/167, 2014).

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit mediaanddemocracy.com for more information.

This report was supported by a grant from Luminate.