# THE INTERSECTION BETWEEN CYBERCRIME LAWS AND DATA PROTECTION LAWS IN THE REPUBLIC OF SOUTH AFRICA

**Njabulo Mthimunye**
BA (SACL)

## INTRODUCTION

The 1st of July 2020 is an important date for South African law, specifically within the context of Cyber Law. This is the date on which both the Cybercrime Bill 2017 was passed by the National Council of Provinces, as well as the date on which the Protection of Personal Information Act No. 4 of 2013 (the 'POPIA') was effected. The two pieces of legislation are mutually exclusive in that they regulate separate issues which are of concern and importance to all South Africans.

## THE PURPOSE OF THE CYBERCRIMES BILL AND THE POPIA AS CYBERLAW INSTRUMENTS

The importance to be attributed to each statute may be gleaned by looking into the purpose for which the respective statutes were created. The Cybercrime Bill is an Act aimed at *inter alia* creating specific offences that have a bearing on cybercrime as well as pronouncing the consequences for such offences, and to impose obligations for the reporting of cybercrimes. The POPIA on the other hand, is statute aimed at *inter alia* promoting the protection of personal information processed by private and public bodies, and to provide for the establishment of a custodian named the Information Regulator to exercise powers in terms of the POPIA and the Promotion of Access to Information Act No. 2 of 2000 (PAIA).

Issues surrounding the ordinary person's safe maneuver of the internet are directly impacted by both pieces of legislation and as such it is not only important to have a basic understanding of their core tenets, but to also briefly investigate any possible overlap between them. With a plethora of publicly available opinions and scholarly articles on the relevant provisions of the Electronic Communications and Transactions Act No. 25 of 2002 (the 'ECTA'), this article accordingly deals with its relevance in so far as specific provisions of the Cybercrimes Bill replace those of the ECTA.

The provisions included in this discussion therefore include the provisions relating to hacking, unlawful interception of data, ransomware, cyber forgery and uttering, and cyber extortion. The provisions discussed here from the POPIA include safety and security safeguards, direct marketing and the principles to be observed by private and public bodies when processing personal information.

**THE OVERLAP BETWEEN THE ECTA, THE CYBERCRIMES BILL AND THE POPIA**

The need for a creation of a coherent system of cyber laws in South Africa has clearly been identified by the legislature. This is demonstrated firstly by the development of a number of statutes, each with a particular focus on protecting interests in the use of the internet and secondly by the existence of a stand-alone regulation of safety and security safeguards in the POPIA where the Cybercrimes Bill presents some gaps or *lacunae* in the law. The specific wording used in the Memorandum on the objects of the Cybercrimes Bill to demonstrate this submission is as follows:

> "Critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002), narrowly caters for the protection of databases only and not for other information infrastructures which need to be protected. No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with those standards."

Chapter XIII of the ECTA is entitled 'Cyber Crime' and regulates unauthorized access to, interception of or interference with data; computer-related extortion, fraud and forgery; attempt at aiding and abetting; and set out penalties for persons convicted in relation to particular provisions of the ECTA. The Schedule contained at Section 61 of the Cybercrimes Bill sets out the sections of the ECTA to be repealed upon the Cybercrimes Bill becoming passed into law, or as an Act of Parliament.

It is important to note that while the 1st of July 2020 is indeed a crucial date for the Bill as a legal instrument, the Bill only comes into full operation, force and effect once signed and assented to by the President of the Republic of South Africa.The provisions specified as being repealed in terms of the Schedule of the Cybercrimes Bill include sections 85 – 89 of the ECTA.

Of particular relevance to this discussion is Section 86 of the ECTA which contains an anti-hacking provision [Section 86(1)], unlawful interference with data [Section 86(2)], an anti-cracking provision [Section 86(3)] and unlawfully overcoming security measures using a computer or device [Section 86(4)]. The latter provision of the ECTA provides that "*a person who utilizes any device or computer program … in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence*." There is clearly an inherent acknowledgement in this provision that cybercriminals make it their duty to overcome security measures put in place to protect data.

The word 'data' is clearly defined in the ECTA. The same wording is used in the Cybercrimes to Bill define data as "electronic representations of information in any form". The POPIA does not directly offer a definition of 'data', however, it provides an extensive definition of what actually constitutes 'personal information'. It is therefore clear that the ECTA and the Cybercrimes Bill offer a wide definition for what constitutes data, whereas the POPIA, although offering a wide enough definition in its own right, remains specific to information of a personal nature.

What is in fact unique about the POPIA as a piece of South African legislation compared to foreign laws or international legal instruments is its reference to 'personal information', whereas foreign laws such as the European Union General Data Protection Regulation refer to 'personal data'. The meaning of 'information' is nevertheless synonymous with 'data' in the context of South African cyber law. It is submitted therefore that where the ECTA and the Cybercrimes Bill refer to data, and where the law would necessarily require a consideration of either statute alongside or against the POPIA, the word 'data' as used in the ECTA and the Cybercrimes Bill has a similar meaning to the word 'information' used in the POPIA.

From the above submissions it becomes patently clear that cybersecurity laws place negative obligations on individuals to refrain from breaching security measures taken to protect data. From a data protection perspective, however, there is also a positive duty on private and public bodies to put in place safety and security safeguards to protect and maintain the integrity of personal information that has been entrusted into their care by persons. It is important at this juncture to briefly highlight the stakeholders in discourse on data protection as envisaged by the POPIA.

For the sake of clarity, the example we use in this article is that of a relationship between a bank and a person who uses the services of such a bank. For the purposes of POPIA therefore, without delving into an academic discussion, suffice it so state that a banking institution is typically a private body that is considered a 'responsible person' that processes its clients' personal information; any third party to whom the bank may outsource work involving the processing of such personal information is considered an 'operator'; and a data subject, which would be either a natural person (a human being) or a juristic person (a legal entity such as a private company) whose personal information is processed.

The positive duty placed upon responsible parties in terms of the POPIA is contained in Chapter 3 thereof, which broadly sets out the conditions for the lawful processing of personal information. The conditions are specified from Sections 8 – 25 as Accountability, Processing Limitation, Purpose Specification, Further Processing Limitation, Information Quality, Openness, Security Safeguards and Data Subject Participation. Condition 7 (seven) of the POPIA provides for security safeguards in Sections 19 -22 and such regulates the security measures on integrity and confidentiality of personal information; information processed by an operator or a person acting under authority; security measures regarding information processed by an operator; and notification of security compromises.

The positive duty placed upon responsible parties in Section 19(1) of the POPIA expressly states that "*A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information*." Section 19(2) specifies that in order for this to be achieved, it is a lawful obligation, buttressed by the use of the word 'must', for the responsible parties to "*take the reasonable measures to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards*."

With the use of the example of banking institutions above, it can be concluded that a bank is legally obligated to ensure that its clients' personal information is processed in a manner that remains in keeping with data protection laws. Although the subject of another discussion, it is noteworthy that the right to privacy as contained in Section 14 of the Constitution of the Republic of South Africa is to be respected by responsible parties such as banks. That is to say that in processing personal information – which may include storage, maintenance, dissemination to operators (i.e. for the purposes of direct marketing of further products and services such as life insurance or assistance with the attestation to a will through the bank), banks are called upon to put in place security safeguards.

In the event that there is a cybersecurity or data breach of its systems, the POPIA creates an obligation for responsible parties to report same with the Information Regulator as well as with data subjects as spelled out by Section 22 of the POPIA. Where an overlap between the ECTA, the Cybercrimes Bill and the POPIA becomes evident lies in the fact that security measures to be taken by responsible parties will include computer software including efficient anti-virus software and firewalls, hardware and management of the way in which persons employed by responsible process personal information whether in electronic format, physically on paper or otherwise. Accordingly, in the event that such security measure is overcome by a cybercriminal, the Cybercrimes Bill imposes consequences.

**CONCLUSION**

The Cybercrimes Bill is an important piece of legislation within the field of cybersecurity law. Its coming into effect takes over some important provisions which the ECTA has regulated in the past. The POPIA, although not strictly considered as an aspect of cybersecurity, but rather as a piece of legislation focused at data protection, overlaps with the Cybercrimes Bill insofar as the latter relates to obligations surrounding security safeguards to be put in place by private or public bodies processing personal information, or conversely to be respected and not compromised by other persons. The coherence of cybersecurity and data protection laws in the advent of 4IR are of premium importance in that methods to overcome security systems as well as the compromising of personal information for sinister purposes are in a dynamic and constant state of evolution.

**REFERENCES**


1. Cybercrimes Bill, 2017.
2. Electronic Communications and Transactions Act No. 25 of 2002.
3. Promotion of Access to Information Act No. 2 of 2000.
4. Protection of Personal Information Act No. 4 of 2013.