Exploring South Africa's Cybersecurity Legal Framework Regulating Information Confidentiality, Integrity, and Availability

Murdoch Watney
University of Johannesburg, South Africa

mwatney@uj.ac.za

Abstract: Globally the digital ecosystems of all countries face a common denominator, namely the threat of cyber operations and how to respond effectively to the threat. There are various types of cyber operations, but the discussion focusses on the national cybersecurity legal framework regulating non-state criminal cyber operations that target the confidentiality, integrity, and availability of information. It does not deal with offensive state or state-sponsored cyber operations which fall within the remit of the international law. As Internet access continues to grow and daily life becomes increasingly dependent on Information and Communication Technologies (ICTs), users, institutions, businesses and government are exposed to a variety of cybersecurity threats. The cyberthreats – with specific reference to threats to the confidentiality, integrity and availability of information (data) - are real. For example, one single security breach may result in the exposure of the personal information of millions of people and that exposed information may be used to commit other crimes, such as theft, fraud or extortion. The first line of defense to a criminal non-state cyber operation targeting the confidentiality, availability and integrity of information is a robust and resilient cybersecurity strategy. This strategy must provide amongst others for a cybersecurity legal framework that provides for the: identification of different types of cyber threats to the confidentiality, integrity, and availability of information; and legal response to threats that result in a security compromise (data breach) which also constitutes a cybercrime. The cybersecurity legal framework must provide for the following interlinked key concepts, namely cybersecurity, privacy, data protection, data breach and cybercrime. The discussion will highlight the meaning and relevance of the concepts and the impact of artificial intelligence (AI). It is against above background that the South African legal cybersecurity framework is explored to establish whether it effectively regulates cyber threats targeting information confidentiality, integrity, and availability. Evaluating cybersecurity incidents and the legal response to it may also contribute to a better understanding of the global challenge cyberthreats present to confidentiality, integrity, and availability.

Keywords: Cybersecurity, Privacy, Data protection, Cybercrime, Cyberthreat, Cybersecurity legal framework

1. Introduction

Various entities, such as government, military, corporate, financial, medical facilities and education institutions collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data may be sensitive information, for which unauthorized access or exposure could have harmful and legal consequences (De Groot, 2023). A security compromise impacts negatively on the reputation and trust of the entity, recovering from the data breach has financial implications and the entity may also face legal consequences. In 2023 the average data breach cost for South African organisations reached R49.45 million (Tredger,2023).

As the volume and sophistication of criminal non-state cyberoperations continue to grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, have to take steps to protect personal information (De Groot, 2023; Patterson, 2023). A cybersecurity legal framework that provides for cybersecurity, privacy, data protection, cyberthreat and cybercrime is therefore essential in ensuring the protection of information against non-state criminal cyber operations that specifically target the confidentiality, integrity and availability of information.

For purposes of this discussion, the following South African cybersecurity legislation will be deliberated against the background of the Constitution:

- The Protection of Personal Information Act (POPIA) 4 of 2013; and
- The Cybercrimes Act 119 of 2020.

The discussion explores the effectiveness of the South African cybersecurity legal framework in responding to the threat and risk of a non-state criminal cyber operation that targets the confidentiality, integrity, and availability of information.

2. Understanding the Relationship Between Cybersecurity, Privacy, Data Protection, Cyberthreat, Cybercrime and Impact of Artificial Intelligence (AI)

A government must provide a secure and trustworthy digital ecosystem aimed at protecting information, otherwise a society cannot prosper, nor can the economy thrive. In protecting the digital ecosystem, cybersecurity would be the first line of defence.

Cyber security is an umbrella term that refers to a collection of technical tools, processes, policies, laws, training and awareness programmes etc. that are used to protect systems such as hardware, software and information connected to the internet from threats in cyberspace (Patterson, 2023). The discussion focusses specifically on the legal protection of the confidentiality, integrity and availability of information against cyberthreats.

Section 1 of the South African National Cybersecurity Framework Policy (NCPF) of 2015 defines cybersecurity as:

- The practices of making the networks that constitute cyberspace secure against intrusions;
- Maintaining confidentiality, integrity and availability of information;
- Detecting intrusions and incidents:
- Responding to; and
- Recovering from them.

The concepts, cybersecurity, privacy, data protection, cyberthreat and cybercrime are interlinked. For purposes of this discussion, the term, "intrusion", is replaced with "cyberthreat". Cybersecurity is aimed at protecting privacy and data against cyberthreats, such as unauthorised access to personal information. A cyberthreat may manifest itself in a cybercrime. Cybersecurity consists of pro-active measures aimed at preventing a cyberthreat. Cybersecurity is, however, not infallible and if a security compromise manifests itself as a crime, cybercrime legislation - which is reactive by nature - must provide for the criminalisation of such conduct. A cybercrime may be defined as a criminal offence that is facilitated by or involves ICTs (Watney, 2022).

In terms of South African law, the right to privacy is protected in terms of the common law and section 14 of the Constitution of South Africa 1996. Section 14(d) provides for the non-violation of the privacy of communications. POPIA recognises the right to privacy enshrined in the Constitution and gives effect to this right through mandatory procedures and mechanisms for the collection, use, and processing of personal information. POPIA is essentially, the South African Data Protection Act.

The impact of artificial intelligence (AI) systems in respect of cybersecurity, data protection and cybercrime must be considered. AI systems have advanced and often rely on vast data to train their algorithms and improve performance. This data can include personal information such as names, addresses, financial information, and sensitive information, such as medical records. The collection and processing of this data can raise concerns about how it is being used and who has access to it (ETsystems, 2023). Organisations that deploy security AI and automation extensively experience, on average, nearly R10.49 million lower data breach costs than organisations that do not deploy these technologies (Tredger, 2023). On the other hand, threat actors are also making use of AI (Legodi, 2023).

3. South Africa's Legal Cybersecurity Framework Regulating Information Confidentiality, Integrity and Availability

3.1 Background to the Legal Cybersecurity Framework

Today's digital ecosystem evolves around information. Information has not only become one of the world's most valuable intangible assets, but it is also globally one of the most vulnerable assets (Eldridge et al, 2023). If someone gains unauthorised access to personal information, such information can be used to commit a number of crimes, for example theft, fraud and extortion. It is important that the responsible person has a legal duty to protect personal information and if the responsible party does not comply with the legal duty, it should be held liable. Furthermore, the conduct that compromises the confidentiality, integrity and availability of information as well as the conduct that uses that information to commit other crimes, must be criminalised to ensure the threat actor is held criminally liable.

Prior to the Protection of Information Act 4 of 2013 (POPIA), personal information was inadequately protected in South Africa. South Africa was in dire need to implement data protection legislation to give effect to the constitutional right to privacy. In July 2021, data protection legislation, POPIA, came into effect. It brough South

Africa in line with current international trends and laws on privacy (Malinga, 2023). POPIA is similar to the European Union (EU) General Data Protection Regulation (GDPR).

It does not help to provide for the protection of personal information in accordance with POPIA if the conduct relating to the confidentiality, integrity and availability of information and conduct that uses the unlawfully obtained information to commit crimes are not criminalised. The Cybercrimes Act 19 of 2020 (Cybercrimes Act) which came into effect in December 2021 criminalises not only conduct that contravenes confidentiality, integrity and availability but also conduct relating to the use of such information to commit other offences. For example, the South African pharmaceutical company, Dis-Chem indicated after it had suffered a security breach in 2023, that there was a possibility that the threat actor could use the impacted personal information for further criminal activities such as phishing attacks and e-mail scams (Illidge, 2023). In August 2023, the online newspaper, Daily Maverick suffered a Distributed Denial-of-Service attack (DDoS). It received more than 36 million hits which emanated from a single domain (O'Regan, 2023).

The theoretical interaction between POPIA and the Cybercrimes Act and the relevant statutory sections regarding information confidentiality, integrity and availability will be discussed hereafter at par. 3.2 and par. 3.3 respectively. At par. 4 the practical application of the relevant legislation is deliberated by exploring the legal response to security compromises and whether there are legal shortcomings that necessitate attention.

3.2 Protection of Information Act 4 of 2013 (POPIA)

POPIA (available at https://popia.co.za) and the Regulations relating to POPIA (POPIA Regulations; see https://www.popiact-compliance.co.za/images/Documents/POPIA Regulations - Dec 2018.pdff) are South Africa's primary data protection laws. POPIA provides that a responsible party such as any organisation or person who processes personal information of a data subject must take security measures to prevent unauthorised access, loss, damage, and destruction of personal information. POPIA further provides for the establishment of a data protection authority, the Information Regulator, who is an independent supervisory authority which has been established for the purpose of administering POPIA.

"Personal information" and "processing" are defined in section 1 of POPIA. "Personal information" is "any information relating to an identifiable, living natural person; or an identifiable, existing juristic person" such as education, physical health, mental health, finances, criminal or employment history; ID number, symbol, email address, physical address, telephone number, location or online identifier; names, surname, birth date or beliefs, and biometrics. POPIA has a wide application and impacts all persons processing personal information (Mokdad et al, 2023). "Processing" refers to the "collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of personal information".

POPIA provides eight information protection conditions (principles) that govern the processing of personal information. In terms of condition 7, a responsible party has a legal duty to protect personal information against a security breach, also referred to as data breach or security breach. POPIA does not define a data breach but it constitutes the unauthorised access and disclosure of personal information to a third party without approval. Although condition 7 of POPIA does not stipulate the exact measures that must be taken, it requires that the responsible party must take appropriate and reasonable cybersecurity measures to prevent a loss or compromise of personal information.

Section 22 of POPIA states that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must report the breach to the Information Regulator, and to the data subject. Unlike other privacy laws around the world, such as the GDPR, there is no "harm" or "impact" threshold to trigger a responsible party's reporting obligations under POPIA (Boda et al, 2023). Even if a compromise is unlikely to cause harm or loss to a data subject, reporting obligations still apply. This means that seemingly low-risk events, for example a stolen work laptop but which is subsequently locked by the company's IT department to prevent unauthorised access, or an email containing personal information sent to the wrong person but successfully recalled before being read, fall within the scope of reportable security compromises (Boda et al, 2023). In August 2022, the Information Regulator published a notification template and guidance to facilitate the reporting of security compromises in terms of section 22 of POPIA (see https://inforegulator.org.za/wp-content/uploads/2020/07/Guidelines-on-completing-a-Security-Compromise-Notification-ito-Section-22-POPIA.pdf).

The Information Regulator will investigate if the responsible party had taken reasonable steps to protect the information. If a responsible party is alleged to have committed an offence in terms of POPIA, the Regulator may

issue the responsible person (referred to as the infringer) an infringement notice with instructions to rectify the security compromise. POPIA sets down firm frameworks that organisations have to abide by to avoid fines, criminal prosecution and potential reputation loss. Perpetrators who do not adhere to the enforcement notice can face fines of up to R10 million or 10 years imprisonment, depending on the seriousness of the breach.

Non-compliance with the provisions of POPIA or an enforcement notice may therefore result in the Information Regulator holding the responsible person civilly and criminally liable for a security breach and non-compliance with the enforcement notice. The individuals responsible for the security breach can also face criminal prosecution and conviction and be sentenced to imprisonment for a period not exceeding 10 years (Boda et al, 2023). The data subject can also institute a civil claim against the responsible party for non-compliance with

3.3 Cybercrimes Act 19 of 2020 (Referred to as Cybercrimes Act)

Conduct that affects the confidentiality, integrity and availability of information, such as unauthorised access to information, ransomware attacks, brute force attack and business email compromise (BEC) must be criminalised.

Chapter 2 part 1 sections 2 – 7 of the Cybercrimes Act (available at https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf) provides for crimes against the confidentiality, integrity and availability of information, such as unauthorised access to information; unlawful interception of data, unlawful acts in respect of software or hardware to gain unauthorised access to information or intercept data or unlawfully interfere with data or a computer program or computer data storage or computer system or to unlawfully acquire or use a password to access information. The information obtained in such an unlawful manner can be used to commit other crimes such as those provided for in part 2 sections 8 – 10 and 12 of the Cybercrimes Act, namely fraud, forgery and uttering, extortion and theft.

4. Legal response to a Data Breach and Cybercrime

4.1 Examples of Legal Response

The South African theoretical legislative cybersecurity framework is commendable, but the effectiveness of the legal framework can only be evaluated by means of the legal responses to security compromises.

Since the implementation of POPIA and the Cybercrimes Act, there have been various security breaches. The legal response to the data breach by the responsible party and information Regulator in terms of POPIA and the response by the police to the cybercrime in accordance with the Cybercrimes Act will be explored with reference to various examples.

Example 1: The Information Regulator investigated security compromises at two credit bureaus, namely Experian and TransUnion, which experienced data breaches in 2020 and 2022 respectively (Labuschagne, 2023). TransUnion and Experian are major credit bureaus that hold vast amounts of personal data in their databases. This can include names and surnames, identification numbers, passport numbers, contact information, home addresses, credit histories, dates of birth, vehicle finance contract numbers, and car VINs. Companies and banks use the data to conduct credit vetting on potential customers, as well as other financial background checks.

The Experian data breach occurred in 2020 prior to the implementation of POPIA. It was first reported by the South African Banking Risk Centre (SABRIC) (Labuschagne, 2023). Experian detected the breach more than 50 days after the data had already been transferred (Molosankwe, 2023). The incident exposed as many as 24 million South Africans and nearly 794,000 business entities which dataset the threat actor, Karabo Phungula obtained under false pretences. Phungula allegedly wanted to sell the data for R4 million. He was arrested in 2021, pleaded guilty to fraud and was duly convicted of fraud in 2022 and sentenced to 15 years imprisonment in 2023 (Molosankwe, 2023).

In 2022 TransUnion experienced a ransomware attack. A ransomware attack encrypts data, rendering it inaccessible unless a specified ransom is paid to the threat actor in exchange for decryption (Mostert, 2023). Ransomware attacks pose a serious threat globally, for example in 2021 the United States of America (US) experienced the Colonial Pipeline ransomware attack which severely disrupted its supply chain (Watney, 2022). In 2022 approximately 78% of South African organisations experienced ransomware attacks (Mostert, 2023).

In the TransUnion security breach, the threat actors reportedly obtained personal information of approximately 5 million individuals. A Brazilian hacking group named N4ughtySec claimed responsibility for the security compromise. TransUnion allegedly refused to pay a $15-million (R224 million at the time) ransom to prevent the data being leaked online (Labuschagne, 2023).

Example 2: In September 2021, the Department of Justice and Constitutional Development (DoJ and CD) suffered a ransomware attack on its IT systems, leading to all its information systems being encrypted and unavailable to internal employees, as well as members of the public. As a result of the attack, all electronic services provided by the Department were affected, including the issuing of letters of authority, bail services, e-mail and the departmental website. During the ransomware attack at least 1 200 files containing the names, banking details and contact details of those who had submitted personal information were compromised (Illedge, 2023; Vermeulen, 2023).

On 9 May 2023, the Information Regulator issued an infringement order in which it found that various sections of POPIA had been contravened. The Information Regulator found that the Department had been negligent as it failed to put in place adequate technical measures to monitor and detect unauthorised exfiltration of data from their environment resulting in the loss of approximately 1 204 files. The enforcement notice required the Department to submit proof to the regulator within 31 days of receipt of the notice that the Trend Anti-Virus licence, the SIEM licence and the intrusion detection system licence had been renewed. It also required the Department to institute disciplinary proceedings against the officials who had failed to renew the licences, which were necessary to safeguard the department against security compromises. An enforcement notice is legally binding but in terms of section 97(1) of POPIA, a responsible party may appeal against the enforcement notice. The Department did not appeal against the enforcement notice nor did it comply with the notice within the prescribed time period. As a result of the non-compliance with the enforcement notice, the Information Regulator issued an infringement notice to the Department in July 2023, in which it ordered it to pay an administrative fine of R5 million following its failure to comply with the enforcement notice issued by the regulator on 9 May 2023 (Illidge, 2023; Moyo, 2023; Vermeulen, 2023). The Department became the first institution to be fined for failure to comply with an enforcement notice. In October 2023, the Department indicated that it was challenging both the infringement and enforcement notices (Ndlovu, 2023).

Example 3: In October 2022, eight women were gang raped at an abandoned mine site in Krugersdorp. In order to apprehend the perpetrators, personal information of the victims such as their surnames ages, physical addresses were shared on the police WhatsApp group. Unfortunately, this information was unlawfully disclosed on social media and became public (Goba, 2023). Not only did this unauthorised disclosure cause the victims and family a lot of stress, but it may deter rape victims to report such crime out of fear their information will not be kept confidential. The Information Regulator found that the police had violated POPIA by not taking reasonable security measures to prevent the personal information from being disclosed to the public. In April 2023, the Information Regulator issued an enforcement notice ordering the responsible party to notify the data subjects of the security compromise which relates to their personal information, make a public apology and to investigate how this information was leaked to the public. In May 2023 the police commissioner issued a public apology to the rape victims (see https://www.gov.za/speeches/saps-apologises-krugersdorp-rape-victims-release-their-personal-information%C2%A0-3-may-2023).

Example 4: In May 2023, a well-known South African pharmaceutical company, Dis-Chem experienced a brute force attack (Illidge, 2023). A brute force attack is aimed at cracking a password by continuously trying different combinations until the right character combination is found (Illidge, 2023). On 1 May 2023, Dis-Chem became aware that 3,7 million of its clients' records were compromised when employees received SMS of the breach. It reported the breach to the Information Regulator on 5 May 2023. The Information Regulator issued Dis-Chem with an enforcement notice on 31 August 2023, instructing it to address its security issues or face a R10 million fine. The Information Regulator determined that the responsible party, Dis-Chem had failed to notify its data subjects as required in terms of section 22 of POPIA which the responsible party strongly disputed. It indicated that a formal notice of the security breach had been published on the Dis-Chem website and a media statement had been released nationally. (Mzekandaba, 2023; see https://inforegulator.org.za/wp-content/uploads/2020/07/FINAL-MEDIA-STATEMENT-ENFORCEMENT-NOTICE-ISSUED-TO-DISCHEM-PHARMACIES-LTD.pdf).

4.2 Lessons Learnt From the Legal Response

Globally unauthorised access to personal information and the use of that information for the commission of various types of cybercrime pose a serious challenge to all entities. The examples discussed at par. 4.2 illustrate the type of threats entities face, how they are committed as well as trends or changes in respect of the threats. Furthermore, by evaluating the legal response to security breaches, shortcomings on the side of the responsible party or police may be identified which can be rectified going forward.

South Africa has experienced an increase in cyberattacks on government entities, for example, both the Department of Defence and the State Security Agency (SSA) experienced security compromises in August 2023 The government has a mandate to safeguards its constituents against threats (Mostert, 2023). In this regard, the ransomware attack on the Department of Justice and Constitutional Development (Department) raises serious concerns regarding the manner in which the critical infrastructure was protected and the government commitment to securing the personal information of its citizens. The security breach was the result of negligence of the side of the Department who had not renewed the relevant security software. The Department did not comply with the infringement notice issued by the Information Regulator with the consequence that the Department was fined. Such conduct does not enhance trust that the government is taking its obligation to protect information seriously. Trust can only be ensured through robust internal cybersecurity measures, such as a cybersecurity policy that outlines the entities' data encryption, access controls, incident response, and preventive measures.

Mzekandaba (2023) refers to Jason Jordaan, a principal forensic analyst at DFIR Labs, who has expressed concerns in respect of the enforcement of cybersecurity legislation. Jordaan raises the following 2 points of concern:

- The police who are tasked with the investigation of a cybercrime, such as identifying the threat actor (perpetrator), may not have the relevant investigative experience to effectively investigate a matter, especially in circumstances where the security compromise is committed outside South Africa. For example, the 2022 TransUnion ransomware attack was committed outside South Africa and such cross-border investigation is very challenging despite the Cybercrimes Act read with the Criminal Procedure Act 51 of 1977 providing for the investigation. In many instances, the threat actor is not prosecuted. It is concerning that only an estimated 10% of cybercrime is reported (Kahle, 2023).
- Since the implementation of POPIA, many security compromises have been reported to the Information Regulator who may need assistance in the investigation in establishing whether the responsible party complied with the provisions of POPIA. The Regulator has a dual function and in addition to being the POPIA watchdog, the Regulator also oversees the enforcement of the Promotion of Access to Information Act, 2000 (PAIA) (Boda et al, 2023). South African law requires every organisation to have a PAIA manual available on their website which ensure legal compliance and enhances accountability.

Although above-mentioned concerns are valid, it is not unique to South Africa. The sophistication and number of cyber threats continue to increase which pose a serious challenge to all parties that process personal information on global level (Legodi, 2023).

The 2020 Experian security compromise illustrates that early detection and fast response can significantly reduce the impact of a breach (Tredger, 2023). The Dis-Chem security breach highlights that a responsible party who outsources processing to a third-party provider, will not escape liability. This was also the case when Britain's Financial Conduct Committee (FCC) fined Equifax in October 2023 for a data breach suffered in 2017. The United Kingdom (UK) arm of Equifax had outsourced personal information of British customers to the parent company, Equifax Inc, in the United Nations. FCC found that the UK arm of Equifax had not taken the necessary steps to protect British customers' data (Reuters, 2023).

5. Recommendations

The following is recommended:

- It is commendable that the Information Regulator issued reporting guidelines in 2022, but it should provide a specific time period in which a security compromise must be reported to the Information Regulator.

Article 33 of the GDPR specifies that an organization must report a security breach that affects personal data to a Data Protection Authority (DPA) within 72 hours of becoming aware of the breach (see https://edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach_en). Likewise part 3 of the United Kingdom Data Protection Act of 2018 also provides that organisations must report certain types of personal data breaches within 72 hours of becoming aware of the breach to the Information Commissioner (https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/personal-data-breaches/). The US does not have general federal legislation impacting data protection, but there are a number of federal data

protection laws that are sector-specific which provides for mandatory reporting (see https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa).

- There should be a guideline in respect of paying ransomware. Paying of ransomware should be discouraged. If a company pays ransom, it must be reported to either the Information Regulator or police in order to keep record of payments made.
- The reasons for the lack of reporting cybercrimes must be investigated. Can it be ascribed to the public's mistrust in the police having proper training and investigative experience to deal effectively with cybercrimes (Kahle, 2023)?
- Laws must keep up with technological advancements, such as the use of AI, generative AI and machine learning. South Africa does not have AI specific legislation. Current cybersecurity legislation should give effect to these advancements . POPIA has adopted a "privacy by design" principle which means it embeds privacy into the design. The resulting consequence in dealing with privacy issues is a system that is proactive and preventative, as opposed to reactive or remedial. This design must also take into account technological advancements, such as AI in respect of processing personal information (De Wet and Fourie, 2023; Malinga, 2023). The Information Regulator could issue a code of conduct in respect of the use of AI for personal information processing (de Wet and Fourie, 2023).

6. Conclusion

South Africa's theoretical cybersecurity legal framework provides for the protection of personal information as well as criminal conduct relating to the confidentiality, integrity and privacy of information. Implementation and enforcement of legislation such as POPIA and the Cybercrimes Act may be challenging. Both legislations are relatively new and consequently much can be learnt from exploring the legal responses to cybersecurity compromises. The Information Regulator has made inroads since POPIA came into operation and has taken decisive steps to issue infringement notices to the responsible parties that did not comply with the provision of POPIA. However, the lack of reporting and prosecution of cybercrimes will have to be addressed (Kahle, 2023).

A major challenge facing cybersecurity and privacy laws – not only in South Africa, but globally – is technological advancements and for purposes of this discussion, the legislature has to be cognisant of the impact of AI on cybersecurity, privacy, data protection and cybercrime and to ensure current legislation can adjust to the changes or implement new legislation if necessary.

References

Boda, R et al. (2023) "POPIA enters the terrible twos", [online], https://www.ensafrica.com/news/detail/7266/popia-enters-the-terrible-twos-.

De Groot, J. (2023) "What is cybersecurity? Definitions best practices and examples", [online], https://www.digitalguardian.com/blog/what-cyber-security.

De Wet, PR. and Fourie, J. (2023) "South Africa: AI and data privacy regulations – the complexities of AI technologies and processing personal information", [online], https://vdt.co.za/popia/south-africa-ai-and-data-privacy-regulations-the-complexities-of-ai-technologies-and-processingpersonal-information/.

Eldridge, J et al. (2023) "Cybersecurity and business interruption: foundations for prevention and mitigation", [online], https://www.lexology.com/library/detail.aspx?g=b2a3b8fb-e3dd-4987-9831-74a9934f2969&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=ITechLaw+2015+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-10-06&utm_term=.

ETsystems. (2023) "AI and privacy: The privacy concerns surrounding AI, its potential impact on personal data", [online], https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms.

Goba, T. (2023) "Police violated POPI Act in Krugersdorp gang rape case – Information Regulator", [online], https://ewn.co.za/0001/01/01/police-violated-popi-act-in-krugersdorp-gang-rape-case-information-regulator

Illidge, M. (2023) "South Africa's leak and privacy watchdog cuts its teeth", [online], https://mybroadband.co.za/news/security/506966-south-africas-data-leak-and-privacy-watchdog-cuts-its-teeth.html.

Kahle, C. (2023) "Going beyond 'Nigerian Prince': SA turning into Africa's cybercrime capital", [online], https://www.citizen.co.za/lifestyle/technology/south-africa-turning-into-cybercrime-capital/.

Labuschagne, H. (2023) "South Africa's privacy watchdog investigating data breaches at credit bureaus", [online], https://mybroadband.co.za/news/security/507116-south-africas-privacy-watchdog-investigating-data-breaches-at-credit-bureaus-in-south-africa.html.

Legodi, S. (2023) "Cybercrime files: How AI is making virtual crimes easy and convincing", [online], https://ewn.co.za/2023/10/09/cybercrime-files-how-ai-is-making-virtual-crimes-easy-and-convincing.

Malinga, S. (2023) "POPIA principles must align with AI governance, say experts", [online], https://www.itweb.co.za/content/RgeVDvPRrn8MKJN3.

Mokdad, A et al. (2023) "Q&A: the data protection legal framework in South Africa", [online], https://www.lexology.com/library/detail.aspx?g=28b3e6c1-88d0-4cd4-8b33-4a9fbcfc0d15&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=ITechLaw+2015+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-09-20&utm_term=

Molosankwe, B. (2023) "Gauteng businessman gets 15 year sentence for stealing information from data firm Experian", [online], https://www.news24.com/news24/southafrica/news/gauteng-businessman-gets-15-year-sentence-for-stealing-infromation-from-data-firm-experian-20230330.

Moyo, A. (2023) "InfoReg slaps justice department with historic R5m fine", [online], https://www.itweb.co.za/content/o1Jr5MxPmm2MKdWL.

Mostert C. (2023) "Unprecedented cyberattacks target government entities", [online], https://www.politicsweb.co.za/opinion/unprecedented-cyber-attacks-target-south-african-g.

Mzekandaba, S. (2023) "Information watchdog sees data breaches notifications double", [online], https://www.itweb.co.za/content/j5alrMQAJOQMpYQk.

Ndlovu, (2023) " "Justice department takes Info Regulator to court over R5-million fine", [online], https://techcentral.co.za/justice-department-info-regulator-court/233071/.

O'Regan V. (2023) "India hits Daily Maverick with malicious cyberattack after report on Modi's tantrum", [online], https://www.dailymaverick.co.za/article/2023-08-23-india-hits-daily-maverick-with-malicious-cyberattack-after-report-on-modis-tantrum/.

Patterson, N. (2023) "What is cybersecurity and why is it important", [online], https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security.

Reuters. (2023). "UK watchdog fines Equifax $13, 4 million for role in cyber breach" [online], https://www.reuters.com/technology/uk-watchdog-fines-equifax-134-million-role-cyber-breach-2023-10-13/.

Tredger, C. (2023) "Data breaches cost SA's financial sector R73m on average", [online], https://www.itweb.co.za/content/Olx4zMkazYQv56km.

Vermeulen, J. (2023) "Information Regulator tests its teeth – slaps Department of Justice with R5 million fine", [online], https://mybroadband.co.za/news/security/498859-information-regulator-tests-its-teeth-slaps-department-of-justice-with-r5-million-fine.html.

Watney, MM. (2022) "Cybersecurity threats to and Cyberattacks on critical infrastructure: a Legal Perspective", [online], https://papers.academic-conferences.org/index.php/eccws/issue/view/7.