THE RISK OF AI IN SOUTH AFRICAN CYBERSECURITY

Category: Artificial Intelligence AI,IT Law,Privacy Law and POPIA
written by Ethan Van der Merwe | July 1, 2026

South Africa has been rocked by a large number of cyberattacks against large corporations and government entities this year, and the threat is only increasing. Huge names such as Pick n Pay and Standard Bank have fallen victim to cyberattacks in the past three months, together with government entities such as Statistics South Africa ("**StatsSA**") and the Gauteng Provincial Government. Reports of cyberattacks against South African companies and government entities is becoming an increasingly common occurrence, and this may yet continue in the coming months, if not years, due to the threats of AI in cybersecurity.

A major concern in the increase of cyberattacks is the use of Artificial Intelligence ("**AI**"). In April 2026, Mythos, an AI model designed by Anthropic, through minimal human prompting, found and exploited thousands of software vulnerabilities across major operating systems and web browsers, with an 80% success rate on its first attempt.

The use of AI has now, furthermore, taken an eerie turn. Hackers have begun using AI in their cyberattacks, and South Africans are amongst those who are suffering the consequences.

South African companies and government entities have access to an enormous amount of personal information. The next time you are required to fill in a form or a document which is required by whichever institution you are dealing with, take a step back and consider how much of your personal information you are providing. Names, ID numbers, cell phone numbers, email addresses, and street addresses are often the bare minimum. Additionally, you may be required to provide your Tax Number, banking details, work address and email, along with other personal information. When providing proof of address, how many of us provide our water and lights bills? All this personal information is stored within companies and government entities which are all under increased risk of cyberattacks.

The Protection of Personal Information Act 4 of 2013 ("**POPIA**") regulates the protection of personal information in South Africa. Its purpose is to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party.[1] The Act sets out 8 conditions for the lawful processing of personal information by a responsible party.[2] Of importance to this article is Condition 2: the processing limitation, and Condition 3: the purpose specification, specifically sections 10, 13 and 14.

Section 10 of POPIA, the "minimality" section, states that personal information may only be processed if, given for the purpose for which it is processed, it is adequate, relevant and not excessive. "Adequate, relevant and not excessive" is particularly significant. It calls into question the sheer

volume of personal information we provide to institutions and whether this can be considered "adequate, relevant and not excessive" for the purpose for which it is processed. It would be difficult to argue, for many South African institutions, that the personal information which is sought is not excessive.

Section 13, the "collection for specific purpose" section, states that personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Once more, the question arises of whether the personal information we so often provide to institutions is being collected for a specific, explicitly defined purpose.

Lastly, section 14 considers the retention and restriction of records. It specifically directs that records of personal information must not be retained any longer than is necessary for achieving the purposes for which the information was collected. This provision subsequently raises the question of how long personal information is retained, and how we, as the data subjects, can be assured that such personal information has been destroyed or deleted as set out in section 14(4) of POPIA.

Consequently, to protect the personal information of data subjects, South African companies and government entities ought to conduct a comprehensive review of the personal information it requests and retains. Requesting excessive personal information may constitute a breach of POPIA, as it does not satisfy the 8 conditions for the lawful processing of information, and, furthermore, places South Africans' personal information at a greater risk as a result of the increase of cyberattacks occurring globally and specifically within South Africa.

Of further concern is the cybersecurity mechanisms that are implemented by South African companies and government entities. Unfortunately, for many of these institutions, the cybersecurity policies and mechanisms are reactive rather than proactive. Organisations often lack formal incident response procedures, monitoring, and regular security testing, and when they do have such mechanisms, they are, far too often, established and instituted once a cyberattack has already occurred. Such a pattern represents a further increased risk to South Africans' privacy. Many organisations are not taking proactive steps to enhance their cybersecurity in order to prevent attacks. Instead, we are seeing a pattern of reactive cybersecurity measures being implemented only once an attack has occurred and once there has been a breach of personal information.

For roughly a decade, we have had access to software that focuses on finding a specific class of exploitable vulnerabilities. However, it has never been able to weaponize and exploit such vulnerabilities. That has been something that only human beings have been able to do. To exploit such vulnerabilities, one is required to craft complex programming chains and adapt when these chains fail. This again, is something only humans have previously done. However, this is no longer the case. Ominously, AI has been able to step into the shoes of humans and complete these actions at an astounding rate.

This is a grave threat to South Africans. Over the past months we have seen an increase in cyberattacks against many companies and institutions in South Africa which has exposed the personal information stored by such organisations. In light of the above, we can reasonably conclude that such attacks will only increase.

South Africa's Draft AI Policy has recently been withdrawn due AI hallucinations to found in the footnotes of the Policy. However, due to recent developments, a comprehensive AI Policy is seriously required in South Africa. Regulatory frameworks must be established to prevent the use of AI in future cyberattacks, and greater education on the risks and uses of AI is required. Preventative measures need to be established before AI repeatedly infiltrates our systems.

What is required in South Africa is greater adherence to POPIA, improved cybersecurity measures, and the establishment of a comprehensive AI Policy. Organisations should reconsider the sheer volume of personal information that they require and continuously store. Strict adherence to POPIA regarding the time periods for the storage of personal information and what personal information is collected must occur. Furthermore, organisations must re-evaluate the cybersecurity measures which they employ. Steps should be taken to adopt a far more proactive approach instead of a reactive one, ensuring that risks are mitigated as best they can be. South Africa must take further action to implement its AI Policy and possibly future AI legislation so as to not be left behind. The Department of Digital Technologies, in its Draft AI Policy, stated that it seeks to be a pioneer on the African continent regarding AI regulation. Consequently, we must act with haste to establish a comprehensive Policy to regulate AI and its use in South Africa before we are left behind.

---

[1] Section 2(a) of the Protection of Personal Information Act 4 of 2013.

[2] Section 4(1)(a)-(h) of POPIA.