LEGAL UPDATES 2023:
A YEAR IN REVIEW

PPM
ATTORNEYS

Information Security | Media | Technology | Infrastructure Projects

www.ppmattorneys.co.za

TABLE OF CONTENTS

PPM ATTORNEYS

1. Introduction

As we approach the end of 2023, we, at PPM Attorneys are taking stock of the legal landscape's notable shifts and updates over the past year. We will give you a brief overview of some of the key legal and regulatory developments in the Technology, Media and Telecommunications ("**TMT**") space. Read on for a concise yet comprehensive look at the legal milestones of 2023 and a preview of what to expect in 2024.

2. Privacy and Information Security

2.1. The Information Regulator comes knocking – is your house in order?

2.1.1. In 2023, we saw the Information Regulator ("**Regulator**") ramp up its effort to monitor and ensure compliance with the *Protection of Personal Information Act* 4 of 2013 ("**POPIA**") and the *Promotion of Access to Information Act* 2 of 2000 ("**PAIA**"). The Regulator has been active in ensuring that it monitors POPIA and PAIA compliance by public and private bodies. This highlights the importance for organisations to ensure that they have adequate measures in place to ensure compliance with POPIA and PAIA in order to avoid administrative fines.

2.1.2. POPIA Compliance

2.1.2.1. In April 2023, the Guardian's Fund experienced a data breach which resulted in about R17 million being lost from the fund. The Guardian's Fund is a fund that is aimed at ensuring that money is paid over to heirs of deceased persons, and it is duly administered by the Department of Justice and Constitutional Development ("**DoJ & CD**").[1] The DoJ & CD has since conducted a forensic investigation on the breach and discovered that the Guardian Fund System was breached by the employees and the breach was accordingly reported to the Regulator. We look forward to the Regulator's response to the breach.

2.1.2.2. A record breaking fine for the DoJ & CD was issued on 3 July 2023. This followed after the Regulator issued an infringement notice[2] against the DoJ & CD for contravening certain sections of POPIA. The DoJ & CD has to pay a fine of R5 million for failure to comply with the enforcement notice. The DoJ & CD is taking the Regulator's fine on review.

2.1.2.3. On 31 August 2023, the Regulator issued an enforcement notice[3] to Dis-chem. This follows the finding that Dis-chem was non-compliant with various sections of POPIA. The Regulator found that Dis-chem had failed to ensure that it had measures in place to identify weak passwords, detect unlawful access and it did not comply with the provisions for lawful processing of data subjects' personal information. Dischem, in September, stated that it had since taken all the necessary steps and protocols to comply with the enforcement notice and is working with the Regulator to ensure full compliance.

[1] Media Statement on the fraudulent disbursement of Guardian's Fund Moneys at Master's Office (Pietermaritzburg).
[2] Infringement Notice and R5 Million Administrative Fine Issued to the Department of Justice and Constitutional Development for Contravention of POPIA.
[3] Enforcement Notice issued to Dis-chem due to contravention of POPIA.

2. Privacy and Information Security (cont.)

2.1.2.4. The National Department of Health ("**NDoH**") was referred to the Regulator's Enforcement Committee regarding personal information that was collected during COVID 19. This is after the Regulator made multiple requests to the NDoH to report on how the department is complying with the lawful processing of personal information that was collected. The NDoH's failure to comply with the Regulator's request led to the referral of the matter to the Enforcement Committee for adjudication[4].

2.1.3. PAIA Compliance

2.1.3.1. On 6 October 2023, the Regulator issued a notice which requires public and private bodies to amend their PAIA manuals and to include updated Access Request Forms, an Outcome of Request and of Fees Payable (Form 3). Public bodies are further required to upload the Internal Appeal Form (Form 4). The notice is aimed at ensuring PAIA compliance and website readiness.

2.2. The shifting tide in cybersecurity liability for software

2.2.1. On 2 March 2023, the United States National Cybersecurity Strategy ("**the Strategy**")[5] was published. The Strategy is aimed at creating a safe digital space in the United States. It places a responsibility on organisations that have the capacity and resources to reduce cybersecurity risk, to ensure that there is cybersecurity in the use of technology by American citizens. It seeks to achieve this by shifting the liability onto organisations that fail to put measures in place to ensure that their software is secure. The Biden-Harris Administration is set to work with Congress and the private sector to develop legislation that will establish liability for software products and services. While the Strategy primarily focuses on enhancing cybersecurity within the United States, its implications and global standards can have an impact on other countries, including South Africa. South Africa, as a participant in the global digital economy, may be influenced or inspired to adopt similar strategies to enhance its own cybersecurity posture.

[4] Information Regulator refers National Department of Health to the Enforcement Committee regarding Personal Information collected During COVID-19.
[5] National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov).

2. Privacy and Information Security (cont.)

2.2.2. In April 2023, the Guide on Shifting the Balance of Cybersecurity Risk: Security by Design and Design Principles ("**the Guide**")[6] was issued. The Guide is aimed at providing guidelines and recommendations for best practice regarding cybersecurity for technology manufactures and to ensure that there are minimal vulnerabilities in the technology that is being used. One of the recommendations in the Guide is that manufacturers must take ownership of the security issues of their products. Essentially, manufacturers must invest in mechanisms or measures which will protect their products, which will in turn ensure user protection. By implementing the recommendations from the guide, South African technology manufacturers can contribute to minimising vulnerabilities and ensuring user protection within the country.

[6] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (cisa.gov).

3. Telecommunications

3.1. South Africa's telecommunications regulatory space was relatively subdued in 2023, when compared to 2022. The successful frequency spectrum auction and the publishing of a few draft regulatory documents gave the impression that 2023 was going to be a busy year.

3.2. As contentious as the original September 2022 draft Next Generation Radio Frequency Spectrum Policy for Economic Development ("**the NextGen Spectrum Policy**") was, it was hoped that it would have been finalised and promulgated during 2023. This would have kicked-off proposed sunset provisions for 2G and 3G, freeing up spectrum for 5G use.[7]

3.3. The NextGen Spectrum Policy had not, at the time of writing, been finalised. This is an important policy that liberalises spectrum use and is crucial to promoting objectives like increasing digital inclusion[8] and promoting the digital economy.[9] We do not have any inside information on when the NextGen Spectrum Policy is expected to be published, but there is still a chance that it could still happen this year. Past experience has shown us that it is not unusual for policies like this to be published in late December.

3.4. The year was also punctuated by regular bouts of "Starlink fever". Starlink is SpaceX's satellite internet constellation. The service is able to rapidly, and relatively easily, provide internet access, at good speeds, from some of the most remote locations. Earlier this year, a number of internet service providers ("**ISPs**") started providing the service in South Africa. South Africa's telecommunications regulator, the Independent Communications Authority of South Africa ("**ICASA**"), took issue with this and demanded that the ISPs stop providing the services. ICASA's reason for doing this is that anyone providing internet access in South Africa must have a licence to do so. ICASA went as far as publishing a notice addressing why certain satellite internet services and equipment are illegal, mentioning Starlink specifically.[10]

[7] ShiftinNextGen Spectrum Policy.
[8] Digital Inclusion.
[9] Digital Economy.
[10] ICASA, Illegal provision of or access to satellite internet services and possession, distribution or use of satellite broadband terminals and equipment in South Africa, https://www.ppmattorneys.co.za/wp-content/uploads/2023/12/ICASA-Illegal-provision-of-or-access-to-satellite-internet-services-in-South-Africa.pdf.

3. Telecommunications (cont.)

3.5. As a minimum, an ISP would need to have an electronic communications service ("**ECS**") licence. Depending on how it provides the service, an ISP may also need to have an electronic communications service licence ("**ECNS**") for the infrastructure over which it provides the internet access. ICASA's detractors took issue with this and added fuel to the fire by criticising the Electronic Communications Act's requirement that anyone holding the type of ECS or ECNS licence Starlink requires, would need to ensure that 30% of the equity ownership in the licence holder, would need to be held by people from previously disadvantaged groups.

3.6. There is, of course an element of hypocrisy in this criticism, as restrictions on foreign ownership in the information and communications technology sector is not unusual: Australia, Austria, Belgium, Hungary, Japan and the United States restrict ownership in the telecommunications sector. For example, Israel restricts foreign ownership in the broadcasting sector to 74%. So, ICASA's position is not unusual and if Starlink intends on setting up in South Africa, it will need to comply with South Africa's laws.

4. Media Law

4.1. The RICA Amendments

4.1.1. On 25 August 2023, the RICA Amendment Bill was published following the 2021 AmaBhungane judgment. The judgement ordered that Parliament amend RICA in the following ways:

4.1.1.1. to make provision for post-surveillance notification, whereby its required that notification is made to a person whose communication was intercepted as part of an investigation, after the fact;

4.1.1.2. to make provision for safeguards that address *ex parte* applications for surveillance warrants;

4.1.1.3. to adequately ensure the independence of designated judges;

4.1.1.4. to make adequate provisions that govern the protection of data collected through surveillance or interception; and

4.1.1.5. to adequately protect practising lawyers and journalist who are subject to surveillance or interception.

4.1.2. Accordingly, the RICA Amendment Bill implements the above order by making provision for post-surveillance notifications; providing further safeguards on *ex parte* applications for surveillance warrants; making further procedures regarding the appointment of surveillance judges; making provision for the management of data collection and protection; and protecting practising lawyers and journalists who are subject to surveillance or interception.

4.1.3. The RICA Bill was passed by the National Assembly on 14 November 2023 and transmitted to the National Council of Provinces for concurrence. The RICA Bill is a significant step to correct the deficiencies in RICA, however, it is merely a band-aid approach. We think that further revisions will be necessary to strike a balance between the necessity of surveillance for national security and the protection of individual rights.

4. Media Law (cont.)

4.2. The Competition Commission's Inquiry into Digital Media

4.2.1. On 15 September 2023, the Competition Commission initiated a market inquiry into the distribution of media content on all digital platforms. These platforms include search, social media, and news aggregation platforms. The purpose of the inquiry was for the Competition Commission to examine whether market features on digital platforms impede, distort, or restrict competition against the purports of the Competition Act. South Africa's news media sector is likely to be impacted by the findings from this inquiry, and lead to regulatory changes in the digital media distribution sector. The findings of such an inquiry could potentially lead to recommendations or actions aimed at fostering a more competitive environment.

4.3. Films and Publications Board – Draft Regulatory Instruments on the Obligations of Social Media Companies

4.3.1. On 14 July 2023, the Films and Publications Board published Draft Regulatory Instruments that place certain obligations on social media companies. Amongst others, the Draft Regulatory Instruments makes provision for the prevention of online harm, makes provision for guidelines regulating peer-to-peer video sharing, and makes provision for guidelines regulating harmful content. The regulations are aimed at protecting the public, with a particular focus on children, from being exposed to the online distribution of harmful material. They also aim to prevent and/or mitigate online harm. We anticipate a shift towards to more comprehensive and technologically advanced measures by social media companies to meet regulatory requirements and ensure a safer online environment, particularly for vulnerable audiences.

4.4. Press Freedom – Sithole v Media 24 Judgement

4.4.1. On 2 August 2023, the High Court passed judgement against individuals who were referred to as the "Alex Mafia" by Media 24, journalists, and various other media houses. The media houses were found to have not been gagged previously for the publications they made in the past which constantly referred to the individuals as the "Alex Mafia". The High Court therefore found that granting an interdict or gagging the media after all the previous publications made would be ineffectual. The judgement signifies the victory of press freedom in South Africa, which is rooted in the constitutional right to freedom of speech.

4. Media Law (cont.)

4.5. EEF's Ndlozi v Media24 and Others Judgement

4.5.1. On 19 September 2023, the High Court issued a judgment against Media 24 and its journalists for publishing rape allegations against EFF's Dr Mbuyiseni Ndlozi during the very early stages of police investigations. Although Media24 argued for publication on the grounds of, among others, public interest on the purports of freedom of speech, the High Court ruled that in instances where police investigations are at their very early stages, media houses must be prohibited from publishing information pertaining to the allegations investigated. The High Court upheld the protection of personal information for purposes of confidentiality and protecting a complainant's dignity, as well as for maintaining the integrity of police investigations. The court found that a rape complainant's interest in confidentiality will generally outweigh the public interest in prematurely reporting the alleged crime. The judgment therefore signifies exceptions to South Africa's press freedom and ultimately, freedom of speech rights.

4.6. Resurgence in South Africa's popularity as a film destination

4.6.1. The Department of Trade and Industry provides incentives to boost the local film, television, and post-production industries as an effort to acknowledge their significant economic contribution to South Africa. It is known as the South African Film and Television Production Incentive. The Department has done this to enhance South Africa's reputation as a film-friendly destination. As a result, we see a resurgence of South Africa becoming a popular film-making destination, as filmmakers from overseas have flocked to South Africa to host their productions. For example, Netflix's newest fantasy series "One Piece" was filmed in Cape Town. Moreover, not only is the local film industry supported by the incentives, but employment opportunities in South Africa continue to rise as a result.

4. Media Law (cont.)

4.7. Copyright Amendment Bill and Performers Protection Amendment Bill

4.7.1. In October 2023, the National Council of Provinces and Select Committee on Trade and Industry, Economic Development, Small Business Development, Tourism, Employment and Labour met on a virtual platform to consider the Copyright Amendment Bill and the Performers Protection Amendment Bill. The Bills were passed by the National Council of Provinces and returned to the National Assembly for concurrence. Currently, we await the President's signature for the official implementation of the Bills.

4.7.2. The passage of both bills remains controversial. A number of local and international creative stakeholders including the music and film industries remain opposed to the Bill in its current format. It contains a broad regime of new copyright exceptions and limitations that weakens rights holders' positions in South Africa and curtails contractual freedoms for production projects. The future trajectory of the Copyright Amendment Bill is uncertain with potential legal challenges and debates and the outcome of Constitutional Court proceedings brought by the creative industry will likely shape the direction of copyright legislation and protection in South Africa.

5. Technology Law

5.1. The Race to Regulate Artificial Intelligence

The debut of Generative AI ("**GenAI**") earlier this year triggered many discussions around Artificial Intelligence ("**AI**"). The rise of GenAI has demonstrated the capabilities and benefits of AI, and at the same time, has increased awareness and the risks of deploying AI without proper regulations in place. There has been a growing call for the regulation of AI. Some of the jurisdictions that have steps taken to regulate AI include the European Union ("**EU**"), United States of America ("**USA**"). It also brings about ethical considerations regarding its responsible use. South Africa, like other countries, may need to develop and enforce regulations to ensure the ethical deployment of AI technologies and to address potential biases or discriminatory outcomes.

5.1.1. EU AI Act

5.1.1.1. The European Parliament earlier this year introduced the first regulation on AI, to ensure that AI systems developed and deployed in the European Union are safe, transparent, traceable, non-discriminatory, and environmentally friendly.[11] The EU AI Act establishes and categorises AI systems and practices into different risk levels which include:

5.1.1.2. Unacceptable risk: unacceptable risk AI systems are systems that are considered unacceptable as they contravene EU's values and are a threat to people. They include systems or practices that can manipulate persons or violate vulnerable groups such as children in a manner that is likely to cause harm physically or psychologically.[12]

5.1.1.3. High risk: these are AI systems that may negatively affect the health and safety or fundamental rights of persons. High risk AI systems are divided into two categories and include: AI systems intended to be used as safety component of products; and other stand-alone AI systems with mainly fundamental rights implications whose risks have materialised or are likely to materialise in the near future.

[11] EU AI Act: first regulation on artificial intelligence available at https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
[12] Title II EU AI Act.
[13] Title IV EU AI Act.

5. Technology Law (cont.)

5.1.1.4. Low or minimal risk: AI systems that may pose a low or minimal risk should comply with transparency obligations. Such AI systems include systems that interact with humans, are used to detect emotions or determine association with (social) categories based on biometric data or generate or manipulate content (deep fakes).

5.1.1.5. On 8 December 2023, the European parliament and council negotiators reached a provisional agreement on the AI Act. The co-legislators agreed to prohibit certain applications of AI, which pose a potential threat to citizens' rights and democracy. They also agreed on a series of safeguards and narrow exceptions for the use of biometric identification systems in publicly accessible spaces for law enforcement purposes, subject to prior judicial authorisation and for strictly defined lists of crime. In respect of high-risk AI systems, the negotiators agreed to include a mandatory fundamental rights impact assessment, among other requirements, also applicable to the insurance and banking sectors.

5.1.2. USA AI Executive Order

5.1.2.1. USA President Biden issued an Executive Order on safe, secure, and Trustworthy AI. 'The Executive Order establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition'.[14] It calls for the development of guidelines and best practices for developing and deploying trustworthy AI systems which includes 'developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI.'[15]

5.1.3. South African Artificial Intelligence National Plan

5.1.3.1. The South African government plans to adopt an AI National Plan which will address both generative and applied AI. The adoption of the plan is meant to propel the government to regulate, invest, and promote education around the development and deployment of AI.[16]

[13] Title IV EU AI Act.

[14] The White House 'FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence' available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

[15] The White House 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[16] Department: Communications & Digital Technologies 'Address by Minister Mondli Gungubele on Building an AI-Powered Future for Africa during the Artificial Intelligence Expo Africa 2023' available at https://www.dcdt.gov.za/minister-s-speeches/461-address-by-minister-mondli-gungubele-on-building-an-ai-powered-future-for-africa-during-the-artificial-intelligence-expo-africa-2023.html.

5. Technology Law (cont.)

5.1.3.2. These developments reflect the ongoing efforts to protect the rights, privacy and safety of humans while advancing AI and its benefits. As AI advances and becomes integrated into society, regulating its development and use will continue to be crucial to mitigate and address the risks that tag along with it.

5.1.4. As the rest of world adopts legal and regulatory frameworks to ensure responsible use, it is also crucial for South Africa to develop a strategic approach to AI adoption, considering the specific needs and challenges of the country. Policymakers, businesses, and educational institutions can play key roles in shaping the direction of AI development in South Africa.

5.2. Digital Identity - A single and integrated biometric National Identification System ("NIS")

5.2.1. Earlier this year, the National Identification and Registration Bill 2022 ("**the NIR Bill**") was approved for comments. The NIR Bill among other things aims to establish a single, inclusive and integrated identification database.[17] The introduction and adoption of a single biometric national identification system may have implications on individuals, businesses and government including the following:

5.2.1.1. **Individuals:** the adoption of such a system may simplify identification verification processes when individuals have to access certain activities such as financial transactions. Such a system may also combat identity theft or fraud, however, may raise privacy and data protection concerns on the storage and processing of such personal information.

5.2.1.2. **Businesses:** integrating such a system in a business may reduce or prevent fraud in financial transactions and may also enhance customer's experience as a more efficient and reliable system will be adopted. However, businesses will need to comply with data privacy laws such as POPIA and may need to implement safeguards and security measures to secure a customer's biometric data or personal information.

5.2.1.3. **Government:** The government will have the responsibility to protect the biometric data of citizens by implementing policies and cybersecurity measures that will secure citizens' personal information. The government will also need to ensure that it complies with privacy laws such as POPIA.

[17] The National Identification and Registration Bill 2022 available at https://www.gov.za/sites/default/files/gcis_document/202304/48435gon3311.pdf.

5. Technology Law (cont.)

5.3. Cybercrime Standard Operating Procedures

5.3.1. In October, the South Africa Police Services under Section 26 of the Cybercrimes Act 19 of 2020 published the Standard Operating Procedures ("**SOPs**") that provide a framework for the Search, Access, or Seizure of a Cyber Article for the purpose of conducting investigations related to cybercrimes. The primary objective of these SOPs is to strike a balance between safeguarding the fundamental rights of victims and witnesses while also upholding the rights of a suspect to a fair trial. Under the Cybercrimes Act, a Cyber Article includes data, computer programs, computer data storage medium or a computer system, these types of Cyber Articles can be searched for, accessed and seized without a search warrant.

5.3.2. The SOPs set out clear guidelines for law enforcement officers and agencies in ensuring they act within the bounds of the law when handling cyber-related investigations; and are crucial in regulating and ensuring the effective investigation of cybercrimes.

5.4. Competition Commission final Report on Online Intermediation Platforms Market Inquiry

5.4.1. The Competition Commission published its findings and remedial actions on the market inquiry on Online Intermediation Platforms. The inquiry was initiated on the basis that there are market features of online intermediation platforms that may widen anti-competitive behaviour in that they may impede or distort competition. These findings are likely to shape the regulatory environment for online intermediation platforms, with potential implications for competition, consumer protection and innovation in the digital marketplace.

[18] The Standard Operating Procedures in terms of section 26 of the Cybercrimes available at: https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf.

[19] Competition Commission final Report on Online Intermediation Platforms Market Inquiry available at: https://www.compcom.co.za/wp-content/uploads/2023/07/CC_OIPMI-Summary-of-Findings-and-Remedial-action.pdf.

6. Conclusion

6.1. Thank you for making it to the end of our newsletter. As promised, below are some of our predicted legal and regulatory developments in the TMT sector in 2024.

6.2. Privacy and Information Security

6.2.1. This year we saw the Information Regulator flex its muscles, but just how flexible are those muscles, and can they withstand judicial scrutiny? We will find out as the DoJ & CD takes on the Information Regulator and challenges the legality of the R5 million rand fine issued against it. This looks to be our first POPIA case. We will observe the case as it progresses through the courts and keep you updated.

6.2.2. If anything, the Information Regulator's activities are a reminder about the importance of continuous POPIA compliance by public and private bodies. It is imperative for public and private bodies to understand their obligations in terms of POPIA and PAIA to ensure that they are compliant with the acts and the notices published by the Regulator. This will ensure that they do not face penalties for non-compliance.

6.2.3. In the new year, we expect the Regulator to issue more notices to ensure compliance and make orders on penalties for non-compliance with data protection laws. As we have seen, the Regulator has not been kind to those who are found to be non-compliant so the fines will not be any less hefty than they already are.

6.3. Media Law

6.3.1. Parliament just made it in terms of the deadline to make the amendment to RICA. The National Assembly passed the RICA Bill and it sent to the National Council of Provinces. We will monitor the progress of the RICA Bill through Parliament and keep you updated.

6.3.2. The Competition Commission Media and Digital Platforms Market Inquiry is going full steam ahead, with various stakeholders including big tech, civil society and academia, having made submissions to the inquiry's terms of reference. We will be monitoring the progress of the inquiry in the new year.

6.3.3. The recent judgements related to press freedom and the protection of personal information demonstrates the ongoing challenges of balancing freedom of speech with privacy rights. We are especially interested in seeing more judgements relating to press freedoms which is a constitutionally protected right, as this often sets important precedents on the intersection of media rights, public interest and individual privacy.

6. Conclusion (cont.)

6.4. Telecommunications

6.4.1. 2024 is likely to also see an increase in public private partnerships in the electronic communications sector. There certainly has been more discussion around this approach to projects, with the Minister of Communications and Digital Technologies and his colleagues frequently mentioning the need for such arrangements. There are a number of finance options available which could be used for projects of this nature, for example the USAID blended-finance programme is mobilising an estimated US$455 million in investment capital. Development finance institutions such as the Development Bank of Southern Africa are also likely to finance such projects. Given what we see in the communications sector in South Africa, we believe that 2024 will be much busier year for electronic communications.

6.5. Technology

6.5.1. In 2023, we not only saw the boom in the adoption of AI, but we also saw an increase in activities around AI regulation in different regions. In South Africa, there is still no AI regulatory instrument in place. However, based on the Minister of DCDT's announcement of the soon to be published National AI Plan, organisations can expect to get some guidance on the direction of AI regulation in South Africa.

6.6. That concludes our brief overview of the legal and regulatory developments in the TMT sector. Stay tuned on our social media pages for more updates in the new year.