Sociology Study, Nov.-Dec. 2024, Vol. 14, No. 6, 277-285
doi: 10.17265/2159-5526/2024.06.003

Moving Africa Towards Sustainable Health Systems via the Fourth Industrial Revolution: Balancing Innovation with the Right to Privacy

Ntlahla France
Walter Sisulu University, Mthatha, South Africa

This article explores how the Fourth Industrial Revolution (4IR) can transform and enhance sustainable health systems in Africa, supporting the continent's growth and development goals. The 4IR integrates digital technologies such as Artificial Intelligence (AI), robotics, automation, big data, machine learning, the Internet of Things (IoT), algorithms, and data-driven innovations, offering unique opportunities to address persistent healthcare challenges in Africa. However, this paper will focus specifically on AI systems within the healthcare sector. The paper will investigate how to address AI-related concerns, including privacy rights violations, data exploitation, and the lack of education and training in adopting these advanced technologies in hospitals. The study aims to find a balance between protecting patients' data and privacy through cybersecurity and effectively utilizing AI systems in healthcare. This balance can be achieved by adopting a robust ethical and legal framework that establishes precise data and privacy protection policies, ensuring that AI systems are used responsibly and in compliance with established standards.

Keywords: fourth industrial revolution, artificial intelligence, privacy, data, healthcare sectors

Introduction

The healthcare sector in Africa is a dynamic and diverse part of the economy, poised for significant transformation with the rise of Artificial Intelligence (AI). The Fourth Industrial Revolution (4IR) has introduced AI technologies that are revolutionizing healthcare globally, and Africa is no exception. Both public and private healthcare sectors are beginning to embrace these innovations to improve patient services, reduce costs, and enhance patient outcomes—objectives strongly influenced by the global impact of 4IR (Schwab, 2018).

The sector is on the brink of a substantial shift, with AI, automation, and big data set to transform hospitals across the continent. Therefore, van Duin and Bakhshi describe AI broadly as:

> [a] field of science encompassing not only computer science but also psychology, philosophy, linguistics, and other areas. AI is concerned with getting computers to do tasks normally requiring human intelligence. (van Duin & Bakhshi, 2017)

Ntlahla France, currently enrolled for PhD in Law (University of KwaZulu Natal), Master of Laws (University of South Africa), Postgraduate Diploma in Tertiary Education (University of South Africa), Bachelor of Laws (Walter Sisulu University), Professional Legal and Training—Certificate (University of South Africa), National Diploma in Marketing Management (King Sabatha Dalindyebo TVET College). Part-Time Law Lecturer at Walter Sisulu University, Mthatha, South Africa.

Despite various explanations, AI experts have yet to reach a consensus on a specific definition of AI. Therefore, the researcher suggests that a unified definition can only be achieved through interdisciplinary discussions and collaborations facilitated by academic conferences where industry experts share their insights.

Several technological innovations, such as algorithmic management, have emerged in the context of the 4IR. This automation involves replacing human input with machine-driven processes for managerial tasks, significantly enhancing the efficiency of production and distribution activities (Filippi, Bannò, & Trento, 2023). These innovations will improve patient services by enabling hospitals to manage and treat a larger number of patients compared to when these tasks were solely reliant on human doctors (Matcha, 2023).

The concept of big data refers to “vast, complex, and rapidly growing data sets that surpass the capabilities of traditional data processing tools” (Cloudflare, 2024). These datasets often include both structured and unstructured data. While the term lacks a universally precise definition, it generally describes data sets that are too large and intricate for conventional management tools to handle effectively (Hansen, 2017). In a hospital setting, leveraging big data is crucial for successfully implementing advanced technologies. For these innovations to function optimally, they require access to a wealth of patient information, including those who will benefit from these innovations. This can be achieved by harnessing expansive databases to extract new insights through advanced algorithms, thereby enhancing precision as the data grow and become more accessible (Goves, Kayyali, Knott, & Van Kuiken, 2013).

Many healthcare institutions across Africa are already integrating AI-powered systems capable of autonomously addressing complex healthcare challenges, significantly improving service delivery. These advanced systems can assist numerous patients simultaneously, increasing productivity. For example, while a human surgeon may perform two surgeries per day, AI-driven machines could potentially conduct more than five surgeries without error, all while operating continuously without the need for rest (Harris et al., 2018).

However, challenges arise regarding accountability for harm caused by AI systems in the workplace. For example, at Stanford University in the United States, an AI system was deployed to distribute COVID-19 vaccines, prioritizing frontline workers like doctors and nurses. However, the AI system failed, misdelivering vaccines and leaving some frontline workers unvaccinated. This raises questions about who should be held responsible in such circumstances (Guo & Hao, 2020).

While AI in healthcare presents numerous benefits, it also introduces significant risks, mainly due to the lack of regulation surrounding these technologies. One primary concern is data privacy and security. Data privacy and security are significant concerns, as AI systems often require access to vast amounts of patient and healthcare worker data, raising the risk of exploitation and misuse. This raises critical questions about accountability in the event of data breaches or unauthorized data usage. Another concern is the potential for AI systems to make incorrect diagnoses or prescribe incorrect treatments, which could have profound implications for patient safety.

Additionally, there is a pressing need for technological education among healthcare practitioners. As AI becomes more integrated into healthcare systems, healthcare professionals must be adequately trained to use these technologies effectively and safely. With proper education and training, the potential benefits of AI in healthcare may be fully realized, and the risks could outweigh the advantages.

While AI and other 4IR technologies have the potential to revolutionize healthcare in Africa, careful consideration must be given to the challenges they present. Ensuring proper regulation, safeguarding data privacy, and investing in the education and training of healthcare workers are crucial steps to maximizing the benefits of these technological advancements while minimizing their risks.

Ultimately, this paper explores the issues that may arise from adopting AI systems in the healthcare sector. Based on the findings, the healthcare sector must strike a balance to protect those involved with AI systems, ensuring that their data are not exploited and that their right to privacy is upheld at all times while utilizing these machines.

Insufficient Technological Education and Training in the Healthcare Sectors

The rapid advancement of AI presents both opportunities and challenges across industries. One of the significant issues is the need for more knowledge and skills, which may lead to AI systems replacing human workers. This is because many workplaces are replacing skilled employees with AI for efficiency (Morandini et al., 2023). Hence, continuous training and skill enhancement are needed to sustain worker productivity (Gleason, 2018). Advocate for innovative lifelong learning, upskilling, and reskilling programs to help individuals adapt to changing labour market demands (Brühl, 2015). Since proper education allows individuals to effectively use and manage AI technologies, their career prospects are limited, and socioeconomic disparities are exacerbated.

The lack of preparedness in AI education can exacerbate existing inequalities, particularly affecting marginalized and disadvantaged communities facing barriers to advanced education and training. Therefore, higher education must develop human capital, but it raises concerns about institutions' ability to meet current demands. Academic practitioners argue that universities must update curricula to align with evolving workforce skill requirements (Samuel & Moagi, 2022).

Inadequate training can also impede technological progress, affecting overall productivity and innovation. As a result, insufficient AI education could worsen inequalities in South Africa, particularly affecting unskilled and low-income individuals and limiting their advancement opportunities (Shivdasani, 2019). This lack of AI skills disproportionately affects marginalized communities, worsening their socioeconomic disadvantages and limiting workforce advancement opportunities.

For example, the Department of Basic Education is working to integrate AI into the grade R curriculum to introduce technology at an early age (Department of Basic Education, 2024). This highlights the importance of lifelong learning and the value of both young and older employees in adapting to virtual jobs (Stock-Homburg, 2013). Additionally, customized AI education and training are needed to ensure that workers acquire the necessary skills and remain competitive (Hecklau, Galeitzke, Flachs, & Kohl, 2016).

Therefore, healthcare sectors need to implement strategies to equip their workers with the necessary education to prevent job losses and prepare for the future of healthcare. These strategies should also ensure that future workers have fair access to AI knowledge while considering legal and ethical frameworks.

Data Protection and Cybersecurity

AI systems operate through data, which are received from specific individuals. It is vital to control those affected, such as workers and patients, as well as those in management positions in the hospital, to address the imbalance in the AI systems regarding the right to privacy and promote a new digital philosophy (Colclough, 2021). Healthcare sectors must adopt data analytics and machine learning, which will assist in data security (Firican, 2020). With data analytics and machine learning, healthcare industries can significantly improve their data security protocols, safeguarding sensitive patient and employee data from advanced cyber-attacks (An, Rahman, Zhou, & Kang, 2023). Incorporating AI into these procedures enhances the capacity to identify, react to, and stop data breaches, guaranteeing healthcare institutions' secure and efficient operation.

AI systems present many glimpses and glamour. However, there are many reasons; for example, in circumstances where data might be leaked about a particular patient in the hospital, who will be accountable for such conduct? Similarly, when one decides to disclose it to an outsider, most of the data in hospitals are generated among workers, such as doctors, nurses, and pharmacists (Hong et al., 2018). Therefore, a similar question arises about who should blame since these technological devices are unregulated.

Cybercrimes targeting AI systems are a growing concern as AI becomes more integrated into critical industries (Guembe et al., 2022). These crimes can include attacks that manipulate AI algorithms, exploit vulnerabilities in AI infrastructure, or use AI to conduct sophisticated cyberattacks. The risks range from data breaches and identity theft to the corruption of AI-driven decision-making processes, potentially leading to significant financial, operational, and reputational damage. As AI systems become more complex and widespread, it is essential to develop robust cybersecurity measures to protect them and the data they handle, ensuring their reliability and trustworthiness.

These issues highlight the need for voluntary consent, the option to opt out, restrictions on data collection, clear explanations of how AI processes information, and the ability to erase data upon request. Often, patient data are collected through AI systems without their awareness, leading to unintended consequences, including patients seeking to remove their data from the hospital after it has been used (Pearce, 2021).

The healthcare sector must proactively protect worker and patient data by implementing comprehensive security measures (Protected Trust, 2020). This includes adopting strong encryption to safeguard data at rest and in transit and deploying continuous monitoring systems to detect and address suspicious activities or breaches in real-time. Regular risk assessments are essential for identifying and mitigating system vulnerabilities. Employee training in data security practices is crucial for identifying potential threats and response strategies. Strict access controls, including multi-factor authentication, should be enforced to limit data access to authorized personnel.

A robust incident response plan is necessary to effectively address and contain data breaches. Collaboration with cybersecurity experts is also essential to stay current with emerging threats and best practices.

Healthcare's Privilege to Utilize AI Systems and the Duty to Safeguard Privacy Rights

Technological advancements in the Fourth Industrial Revolution (4IR) have increasingly blurred the lines between patients' privacy rights and the healthcare sector, leading to profound changes in the workplace[1]. While the Constitution safeguards individuals' privacy rights, the integration of AI systems has introduced complexities that challenge these protections. The researcher believes that there must be an ethical and legal balance between the benefits healthcare providers derive from leveraging AI systems and their obligation to respect and protect patients' privacy. It examines how AI adoption in healthcare enhances diagnostic accuracy, treatment efficiency, and operational workflows but simultaneously exposes sensitive patient information to significant risks.

[1] Section 14 of the Constitution of the Republic of South Africa, 1996, protects the right to privacy. However, this right is not absolute and can be limited under Section 36 of the Constitution.

The quick growth of AI in workplaces brings up significant concerns regarding data privacy, as gathering and utilizing personal data can lead to potential misuse and privacy infringements. AI's growing presence in the workplace has led to complex data and privacy issues (Papadopoulos & Snail, 2012). Although, privacy and data protection are essential ethical considerations (Frank et al., 2024).

However, it is difficult to define the concept of privacy in the workplace due to the use of AI technology. This challenge has resulted in the difficulty of defining privacy in legal terms (Posner, 1978). However, the current legal definitions of privacy are frequently overly inclusive or restrictive (Solove, 2006). While no widely agreed-upon definition exists, safeguarding personal information has been highlighted as technology progresses (Solove, 2004).

The COVID-19 outbreak continued to push the limits of privacy as countries put in place strategies to monitor people's actions to control the spread of the virus. This increased monitoring has sparked worldwide worries regarding privacy rights and the responsibility of such actions (Almeida, Shmarko, & Lomas, 2022). Many employees had their privacy rights violated during the pandemic, with AI surveillance monitoring them without consent, even in their own homes. However, this unauthorized surveillance shows how AI technology can breach employee privacy, causing frustration (Otto, 2016) and dissatisfaction among workers (Moussa, 2015).

On the other hand, overseeing can improve efficiency (Van Jaarveld, 2004). Using AI systems in hospitals should be approached with care and prudence. The government needs to understand that workers might be retaliated to work with AI systems if they believe that the adoption becomes unfair, especially since these advanced technological devices are unregulated.

This paper seeks to address the privacy challenges posed by AI technology, focusing on key aspects such as obtaining informed consent, the right to opt out, limitations on data collection, transparency in AI processes, and the ability to delete personal data upon request. It highlights the need to balance employees' privacy rights with employers' legitimate interests in monitoring workplace resources.

The analysis underscores the responsibility of healthcare institutions to comply with privacy laws and ethical standards, ensuring that AI implementation aligns with principles such as confidentiality, informed consent, and data minimization. Additionally, it explores potential conflicts between technological advancements and the rights protected under frameworks like the National Health Act and data protection regulations. The study advocates for robust mechanisms to safeguard privacy in AI-driven healthcare environments while fostering ethical innovation.

Existing Legal and Ethical Frameworks Governing AI Systems in the Healthcare Sector

Although several countries have initiated efforts to establish AI policies, the regulation of AI systems remains largely inconsistent and underdeveloped on a global scale, for instance, countries like China (Xaltius, 2019), the United Kingdom (Elman & Castilla, 2017), and the United States of America (OSTP, 2016). These countries are regarded as front-runners in discussing these concerns and have already begun to make provisions for interventions to regulate AI systems for businesses (Eke, Wakunuma, & Akintoye, 2023).

In contrast, South Africa lags in developing and enforcing AI-specific policies, particularly within the healthcare sector. This section outlines regulatory frameworks that South African regulators and policymakers should consider when crafting AI policies tailored to healthcare.

The paper will examine the existing legal and ethical frameworks governing AI in the healthcare sector, including the National Health Act, data protection legislation, and international guidelines. It explores how these frameworks address critical issues such as patient safety, data privacy, and accountability in AI applications.

The analysis identifies significant gaps, such as the absence of provisions specific to AI-driven decision-making, the risks of algorithmic bias, and the need for transparency in AI processes. Ethical principles such as beneficence, non-maleficence, autonomy, and justice are also evaluated for their role in promoting equitable and ethical AI integration.

The section concludes by highlighting areas where legal and ethical standards must evolve to keep pace with rapid technological advancements, ensuring that AI adoption in healthcare aligns with both innovation and patient-centred care.

Protection of Personal Information Act (hereafter—POPIA)

AI systems must comply with South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) to regulate issues related to the privacy and protection of personal data. POPIA is the primary legislation for safeguarding personal information, establishing strict conditions for lawful data processing (Mostert & Tembedza, 2020). This includes the obligation for hospitals and healthcare providers to securely store patient data and ensure that it is used solely for its intended purposes (Newman, 2022). The healthcare sector must understand the limitations and responsibilities of using AI in handling workplace data, especially in light of the global increase in unethical data practices, invasive surveillance, and privacy violations (Firican, 2020).

As data security breaches become more common due to the rise of data analytics and machine learning within AI, healthcare providers must be well-versed in regulations governing data input into AI systems (Zhang et al., 2022). POPIA grants patients the right to access their data and mandates that any data breaches should be reported to relevant authorities and affected individuals. Businesses must establish robust plans and policies, including in contracts, to ensure compliance with POPIA on all platforms (Data Privacy Manager, 2024).

Additionally, hospitals must consider patients' privacy rights when developing such policies[2]. Compliance with POPIA is essential for any AI system used in South Africa, and careful consideration of the Act's provisions is required when designing AI solutions for healthcare sectors[3].

The 4IR offers immense potential to advance healthcare in South Africa but also presents significant challenges to patient privacy. Hospitals must adhere to legal frameworks like POPIA, implement robust data protection measures, and maintain a solid commitment to ethical practices to navigate these challenges. By doing so, they can leverage the benefits of 4IR technologies while safeguarding patients' privacy rights, ultimately enhancing trust and improving healthcare outcomes.

National Health Act (hereafter—NHA)

The advancement of AI systems in healthcare has the potential to significantly improve patient services, particularly in regions like Africa, where there is a well-documented shortage of healthcare staff due to a

[2] Section 14 of the Constitution of the Republic of South Africa.

[3] These provisions are set out by section 57(1), section 57(1) (a) (i) (ii), and section 57(2) of the Personal Information and Privacy Act of 2013.

rapidly increasing population. However, the lack of regulation surrounding these advanced technologies poses risks to the healthcare sector.

Therefore, it is imperative to establish regulatory frameworks that specifically address the integration of AI in healthcare. Such regulations will help determine accountability for any harm caused by AI systems, clarifying whether liability should rest with the manufacturer or the user of the AI system without stifling innovation.

Moreover, regulators must consider the National Health Act (NHA) provisions[4]. This Act governs healthcare practices, including protecting patient privacy and the confidentiality of their information, which must not be disclosed without consent unless the healthcare practitioner can justify the need for disclosure (Health Professions Council of South Africa, 2021). Practitioners ensure that all staff, including clerks and receptionists, adhere to confidentiality standards (Peters, 2019).

When a healthcare provider determines that information should be disclosed, they must act promptly to release all relevant information, especially when it is essential to protect the patient's best interests or to safeguard others' well-being (General Medical Council, 1999). The guidelines on confidentiality, developed through extensive consultation with professional and patient groups, are aligned with the NHA. They place a clear responsibility on healthcare practitioners to obtain consent and keep patients informed about disclosing their information.

Therefore, the government should take into consideration when implementing legal and ethical frameworks regarding AI systems for healthcare sectors.

Conclusions

The 4IR is ushering in a significant transformation in healthcare services. Advanced technological machines introduced by 4IR operate faster and with fewer errors than human workers. Embracing these innovations can enhance efficiency and reliability in healthcare delivery, as these devices do not experience fatigue and can handle tasks traditionally performed by human practitioners. This shift may alleviate workload pressures and reduce instances where staff must forego breaks due to staffing shortages.

To ensure these technologies' responsible and effective integration, healthcare sectors must implement clear policies regarding patient data usage. Patients should be fully informed about how their data will be utilized by these advanced devices, maintaining transparency and trust in the healthcare system. Healthcare practitioners must be educated on properly using these technologies and understand the consequences of misuse, including disciplinary actions or termination. Establishing boundaries is essential to prevent the exploitation of these devices for personal gain and to safeguard the privacy and value of patient data.

According to World Health Organization (2013), it provides that there should be a regular training and workshops recommended to keep healthcare workers informed and compliant with current legal and ethical standards. These educational initiatives should be conducted biannually or annually, providing updates on policy amendments and offering opportunities for practitioners to contribute to developing and improving AI-related policies. Such engagements ensure that healthcare professionals remain aligned with best practices and understand the implications of violating established guidelines.

[4] National Health Act 61 of 2003.

Given the evolving nature of technology and its impact on healthcare, the researcher proposes collaborative efforts among diverse stakeholders affected by the 4IR. This includes political leaders, businesses, social leaders, policymakers, academics, and government officials working together to create a harmonious work environment and build confidence among patients interacting with these advanced devices. Collaborative policymaking and cross-sector partnerships are essential to effectively regulate technological advancements and ensure that they serve the best interests of all parties involved.

References

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics, 2,* 377-387.

An, Q., Rahman, S., Zhou, J., & Kang, J. J. (2023). A comprehensive review on machine learning in healthcare industry: Classification, restrictions, opportunities and challenges. *Sensors, 23*(9), 4178.

Brühl, V. (2015). *Economy of the 21st century: Challenges in the high-tech economy*. Wiesbaden: Springer Professional Media.

Cloudflare. (2024). *What is big data?* Retrieved from https://www.cloudflare.com/learning/ai/big-data/

Colclough, C. (2021). *Towards workers' data collectives: A digital new deal*. Retrieved from https://projects.itforchange.net/digital-new-deal/2020/10/22/towards-workers-data-collectives/

Data Privacy Manager. (2024). *Introduction to POPIA: South Africa's data protection law*. Retrieved from https://dataprivacymanager.net/introduction-to-popia-south-africas-data-protection-law/

Department of Basic Education. (2024). *Curriculum and Assessment Policy Statement (CAPS) Coding and Robotics Foundation Phase Grade R-3*. Retrieved from http://www.education.gov.za

Eke, D. O., Wakunuma, K., & Akintoye, S. (2023). *Responsible AI in Africa: Challenges and opportunities*. Palgrave Macmillan Cham.

Elman, J., & Castilla, A. (2017). Artificial intelligence and the law. *TechCrunch*. Retrieved from https://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/

Filippi, E., Bannò, M., & Trento, S. (2023). Automation technologies and their impact on employment: A review, synthesis and future research agenda. *Technological Forecasting and Social Change, 191,* 122448.

Firican, G. (2020). *The pros and cons of the 4th industrial revolution*. Retrieved from https://www.lightsondata.com/pros-cons-4th-industrial-revolution/

Frank, S., Lessa Derci Augustynczik, A., Havlík, P., Boere, E., Ermolieva, T., Fricko, O., ... Wögerer, M. (2024). Enhanced agricultural carbon sinks provide benefits for farmers and the climate. *Nature Food, 5*, 742-753.

General Medical Council. (1999). *Disclosing patients' personal information: A framework*. Retrieved from https://www.gmc-uk.org/professional-standards/the-professional-standards/confidentiality/disclosing-patients-personal-information-a-framework#

Gleason, N. W. (2018). *Higher education in the era of the fourth industrial revolution*. Palgrave Macmillan, Singapore.

Goves, P., Kayyali, B., Knott, D., & Van Kuiken, S. (2013). *The 'big data' revolution in healthcare: Accelerating value and innovation*. Center for US Health System Reform, Business Technology Office. Retrieved from https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Healthcare%20Systems%20and%20Services/PDFs/The_big_data_revolution_in_healthcare.ashx

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence: An International Journal, 36*(1), 2037254.

Guo, E., & Hao, K. (2020). This is the Stanford vaccine algorithm that left out frontline doctors. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2020/12/21/1015303/stanford-vaccine-algorithm/

Hansen, S. (2017). *How big data is empowering AI and machine learning?* Retrieved from https://hackernoon.com/how-big-data-is-empowering-ai-and-machine-learning-4e93a1004c8f

Harris, L., Hamilton, S., Azevedo, L. B., Olajide, J., De Brun, C., Waller, G., … Ells, L. (2018). Intermittent fasting interventions for the treatment of overweight and obesity in adults aged 18 years and over: A systematic review and meta-analysis. *JBI Database of Systematic Reviews and Implementation Reports, 16*(2), 507-547.

Health Professions Council of South Africa. (2021). *Guidelines for good practice in the healthcare professions. Confidentiality: Protecting and providing information.* Retrieved from https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic approach for human resource management in industry 4.0. *Procedia CIRP, 54*, 1-6.

Hong, L., Luo, M., Wang, R., Lu, P., Lu, W., & Lu, L. (2018). Big data in health care: Applications and challenges. *Data and Information Management, 2*(3), 175-197.

Matcha, A. (2023). Innovations in healthcare: Transforming patient care through technology, personalized medicine, and global health crises. *International Journal of Science and Research (IJSR), 12*(12), 1668-1672.

Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., & Pietrantoni, L. (2023). The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. *Informing Science: The International Journal of an Emerging Transdiscipline, 26*, 39-68.

Mostert, L., & Tembedza, W. (2020). *Artificial intelligence has POPIA implications*. Retrieved from https://www.webberwentzel.com/News/Pages/artificial-intelligence-has-popia-implications.aspx#:~:text=From%20a%20compliance%20perspective%2C%20businesses%20in%20South%20Africa,must%20be%20considered%20when%20creating%20an%20AI%20system

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *SAGE Open*, 1-13.

Newman, S. (2022). *Privacy matters: How safe is your online data?* Retrieved from https://news.mandela.ac.za/News/Privacy-matters-how-safe-is-your-online-data

Office of Science and Technology Policy (OSTP). (2016). *Preparing for the future of artificial intelligence*. National Science and Technology Council, Washington, D.C. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

Otto, M. (2016). *The right to privacy in employment: A comparative analysis.* Retrieved from https://api.semanticscholar.org/CorpusID:168627868

Papadopoulos, S., & Snail, S. (2012). *Cyberlaw@ SA III: The law of the internet in South Africa*. Van Schaik Publishers.

Pearce, G. (2021). *Beware the privacy violations in artificial intelligence applications*. Retrieved from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

Peters, F. (2019). *The POPI Act vs medical records*. Retrieved from https://www.up.ac.za/media/shared/62/CPD/CPD%202019/Presentations/peters-frank-prof-presentation-popi-act.zp173622.pdf

Posner, R. A. (1978). The right of privacy. *Georgia Law Review, 12*(3), 393-422.

Protected Trust. (2020). *The importance of modern technology in the workplace*. Retrieved from https://www.protectedtrust.com/technology-in-the-workplace/

Samuel, O. M., & Moagi, T. (2022). The emerging work system and strategy for skills transition in South Africa. *Management Research Review, 45*(11), 1503-1523.

Schwab, K. (2018). *The fourth industrial revolution*. Retrieved from https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

Shivdasani, A. (2019). *South Africa's foray into the fourth industrial revolution: Let's learn to walk before we try to fly*. Retrieved from https://www.dailymaverick.co.za/opinionista/2019-07-24-south-africas-foray-into-the-fourth-industrial-revolution-lets-learn-to-walk-before-we-try-to-fly/

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

Stock-Homburg, R. (2013). Zukunft der Arbeitswelt 2030 als Herausforderung des Personalmanagements. In *Handbuch Strategisches Personalmanagement* (2nd ed., pp. 603-629). Wiesbaden: Springer Gabler.

van Duin, S., & Bakhshi, N. (2017). *Part 1: Artificial intelligence defined.* Retrieved from https://www2.deloitte.com/nl/nl/pages/deloitte-analytics/articles/part-1- artificial-intelligence-defined.html

Van Jaarveld, M. (2004). Forewarned is forearmed: Some thoughts on the inappropriate use of computers in the workplace. *SA Mercantile Law Journal, 16*(4), 651-666.

World Health Organization. (2013). *Transforming and scaling up health professionals' education and training: World Health Organization guidelines 2013*. World Health Organization.

Xaltius. (2019). *Countries leading the way in AI*. Retrieved from https://xaltius.tech/countries-leading-the-way-in-ai/

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., & Ghorbani, A. A. (2022). Data breach: Analysis, countermeasures and challenges. *International Journal of Information and Computer Security, 19*(3-4), 402-442.