

AN APPRAISAL OF SELECTED SALIENT HUMAN RIGHTS BEING IMPACTED AND ALTERED BY ARTIFICIAL INTELLIGENCE (AI)

Thupane J Kgoale

LLB LLM

LLD Candidate, School of Law

Faculty of Management and Law, University of Limpopo, Mankweng, South Africa

<https://orcid.org/0009-0009-0863-4861>

Prof Kola O Odeku

LLB LLM MBA LLD

*School of Law, Faculty of Management and Law
University of Limpopo, Mankweng, South Africa*

<https://orcid.org/0000-0003-3132-4545>

SUMMARY

With the emergence and broad deployment of Artificial Intelligence (AI) in all sectors of the economy and human endeavours, this article accentuates the possibility that some fundamental human rights (guaranteed by most civilised nations) will be impacted and altered. To this end, the article appraises selected salient human rights being impacted by the deployment of AI, and which violate protected and guaranteed human rights, raising major concerns. The article assesses the theoretical grounding of human-rights law and its catalytic role in informing and shaping the emergence of new fundamental rights. Equally important, the article delves into pertinent legal issues emanating from the use of AI technologies and their potential threats to vulnerable new rights. While AI promises a significant positive impact on the economy and human development, there is a need to address pertinent concerns about the manner in which AI could impact existing human rights, and ultimately alter the form and content of these rights, resulting in the emergence of new fundamental rights.

1 INTRODUCTION

The key elements underpinning the theory of human rights are ethics, morality and the protection of individual freedoms.¹ Human rights are a set of

¹ Mantelero "AI and Big Data: A Blueprint for a Human Right, Social and Ethical Impact Assessment" 2018 34(4) *Computer Law & Security Review* 754–772.

fundamental rights and freedoms that are inherent, universal and inalienable to a human being.² According to Sen, human rights need not be seen in legal terms, but they serve to inform and inspire laws aimed at protecting such rights and freedoms. In this regard, Sen posits:

“Human rights can be seen as primarily ethical demands. They are not principally ‘legal’, ‘proto-legal’ or ‘ideal-legal’ commands. Even though human rights can, and often do, inspire legislation, this is a further fact, rather than a constitutive characteristic of human rights.”³

While successive industrial revolutions have contributed to the development of numerous technologies, they have also impacted the evolution of international law and, by extension, human rights law.⁴ Transformation in the agriculture industry, the discovery of the steam engine and improvement in industrial operations gave rise to the formalisation and development of human rights theory.⁵ Similarly, the revolutions in mass production, electricity, automation, aviation, radio and telecommunications came with various ramifications for the human rights front.⁶ While the emergence and development of the modern industrial economy from the ancient economy came with its positives, it also had a negative impact on the pertinent fundamental rights enjoyed by human beings.⁷

Expansion in science and new technologies, mobile devices and biotechnology propelled the 3rd Industrial Revolution (3IR).⁸ The current millennium is described as introducing the 4th Industrial Revolution (4IR) and has witnessed a massive expansion in scientific ideas and methods.⁹ It is predominantly characterised by machine learning, big data, robots, drones, 3D printing, nanotechnology and artificial intelligence (AI), among others. The tone for the 5th Industrial Revolution has been set and will be dominated by advanced computing and the integration of people with collaborative

² Pocar “Some Thoughts on the Universal Declaration of Human Rights and the Generations of Human Rights” 2015 10 *Intercultural Hum Rts L Rev* 43.

³ Sen “Elements of a Theory of Human Rights” 2004 32(4) *Philosophy & Public Affairs* 315–56 <http://www.jstor.org/stable/3557992> (accessed 2023-07-04).

⁴ Stearns *The Industrial Revolution in World History* (2020) 13.

⁵ Sima, Gheorghe, Subić and Nancu “Influences of the Industry 4.0 Revolution on the Human Capital Development and Consumer Behavior: A Systematic Review” 2020 12(10) *Sustainability* 4035.

⁶ Palattella, Dohler, Grieco, Rizzo, Torsner, Engel and Ladid “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models” 2016 34(3) *IEEE Journal on Selected Areas in Communications* 510–527.

⁷ Mokyr, Vickers and Ziebarth “The History of Technological Anxiety and the Future of Economic Growth: Is This Time Different?” 2015 29(3) *Journal of Economic Perspectives* 31–50.

⁸ Mohajan “Third Industrial Revolution Brings Global Development” 2021 7(4) *Journal of Social Sciences and Humanities* 244.

⁹ Skilton and Hovsepian “The 4th Industrial Revolution Impact” 2018 *The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business* 3–28.

robotic systems.¹⁰ Many have also raised concerns about the existential threat posed by AI to human life.¹¹

The Western scientific narrative claims the history, development and discovery of technology and AI for its own scientific community (led by Turing), while no credit is given to its origin in Africa and its diaspora, who have greatly advanced it. The narrative paints the predominantly white male technologists as innovators, while the rest are regarded as beneficiaries of their genius innovations.¹² Africa's contribution to and account of the origin and development of technology and its impact on human rights can be viewed from two angles: first, with the assertion that technology originated in the continent of Africa; and secondly, that the principles and values underlying the *Ubuntu* theory informed the development of human rights.¹³

All over the world, states are integrating and deploying AI systems within their apparatus as part of law enforcement, criminal justice, national security and the provision of other public services.¹⁴ While these AI systems assist in service delivery, they also raise concerns about human-rights issues.¹⁵ Algorithms are key, as they are used in forecasting and analysing large quantities of data to assess the risks and predict future trends.¹⁶ The data in question may relate to crime hot spots, social media posts, communication data or the provision of social services, among others. To complement states' use of AI, corporate companies are at the forefront of manufacturing and producing AI systems, which in turn are traded to public authorities.¹⁷

To mitigate harms and damages arising from the production and deployment of AI systems, this duty entails that states should ensure that their laws respect human rights and that they are applied across all sectors, such as the management of state-owned enterprises, as well as research-and-development funding bodies, including the private corporate companies and vendor.¹⁸ This includes requiring responsible business conduct, including robust due diligence before releasing new AI. A robust due diligence exercise entails overseeing the development and deployment of AI systems by assessing their risks and accuracy before they are brought to

¹⁰ Horn, Rosenband and Smith *Reconceptualizing the Industrial Revolution* (2020) <https://www.tandfonline.com/doi/epdf/10.1080/07373937.2021.1875185?needAccess=true&role=button> (accessed 2023-06-01).

¹¹ Nahavandi "Industry 5.0: A Human-Centric Solution" 2019 16 *Sustainability* <https://doi.org/10.3390/su11164371> (accessed 2023-06-01).

¹² Siyonbola *A Brief History of Artificial Intelligence in Africa* (2021) <https://noirpress.org/a-brief-history-of-artificial-intelligence-in-africa/> (accessed 2023-04-06).

¹³ Gwagwa, Kazim and Hilliard "The Role of the African Value of Ubuntu in Global AI Inclusion Discourse: A Normative Ethics Perspective" 2022 3(4) *Patterns* 2.

¹⁴ Kuziemski and Misuraca "AI Governance in the Public Sector: Three Tales From the Frontiers of Automated Decision-Making in Democratic Settings" 2020 44(6) *Telecommunications Policy* 101976.

¹⁵ Pizzi, Romanoff and Engelhardt "AI for Humanitarian Action: Human Rights and Ethics" 2020 102(913) *International Review of the Red Cross* 145–180.

¹⁶ Sarker "Machine Learning: Algorithms, Real-World Applications and Research Directions" 2021 2(3) *SN Computer Science* 160.

¹⁷ Oatley "Themes in Data Mining, Big Data, and Crime Analytics" 2022 12(2) *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* e1432.

¹⁸ Council of Europe "Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights" (2019) <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64> (accessed 2024/10/02) 7.

market.¹⁹ Equally important is to expect developers, programmers, operators, marketers and other users of AI systems within the value chain to be transparent about the details and impact of systems at their disposal.²⁰ They should in fact go further and inform the public and affected individuals about how AI systems arrive at particular decisions autonomously.²¹ This would also include notifying individuals about the use of their personal data.

It is against this backdrop that the article highlights, with reference to the jurisdictional parameters of South Africa and the European Union (EU), specific international instruments that have direct and indirect impacts on AI. This is juxtaposed with both binding and non-binding international and domestic instruments on selected human rights that are vulnerable to disruptions by AI systems. Guidance is also derived from soft-law principles, which play a critical role in shaping the regulation and governance of AI systems. According to the earlier EU Proposal on AI Act, AI systems are a fast-evolving family of technologies that can bring a wide range of socio-economic benefits across the entire spectrum of the value chain.²² AI systems are regarded as being instrumental in improving prediction and optimising operations and allocation of public goods and resources. The use of AI systems plays a critical role, in supporting socio-economic spin-offs and improving the welfare of people.²³

2 TECHNOLOGICAL GROUNDING OF HUMAN-RIGHTS THEORY

The theoretical background for human rights and their application to AI can be located within the principles underpinning ethics, morality and the broad freedoms to which an individual is entitled. Human rights have been defined as a set of fundamental rights and freedoms that are inherent in all individuals. This is regardless of an individual's nationality, race, gender or other personal characteristics. In particular, these rights include the right to dignity, life, liberty, security, privacy, freedom of thought, expression and many others. Consequently, human rights are said to be inalienable and, as such, inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion or any other status. When it comes to AI, the theoretical background for human rights also involves ensuring that the development,

¹⁹ UN Report of the Special Rapporteur on the Right to Privacy (February–March 2020) A/HRC/43/29 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/66/PDF/G2007166.pdf?OpenElement> (accessed 2023-06-04) par 52.

²⁰ UN Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression (August 2018) A/73/348 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/270/42/PDF/N1827042.pdf?OpenElement> (accessed 2023-06-04) par 49.

²¹ Council of Europe "Guidelines on Addressing the Human Rights Impacts of Algorithmic Systems" (Recommendation CM/Rec (2020)1 of the Committee of Ministers to member states on the human rights impacts of algorithmic systems) section B par 4.2.

²² On 21 April 2021, the European Union Parliament proposed the Artificial Intelligence Act and made proposals for the regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (the Artificial Intelligence Act) and further amending certain Union legislative acts.

²³ Novelli, Bongiovanni and Sartor "A Conceptual Framework for Legal Personality and Its Application to AI" 2022 13(2) *Jurisprudence* 194–219 <https://doi.org/10.1080/20403313.2021.2010936>.

deployment and use of AI systems respect and uphold these fundamental rights. AI technologies have the potential to impact various aspects of human life, including employment, health care, education, and decision-making processes. Overall, the theoretical motivation for applying human rights to AI is based on the recognition that AI should be developed and used in a manner that respects and upholds the fundamental rights and freedoms of individuals, ensuring fairness, transparency and accountability in its design and implementation.²⁴

While the United Nations (UN) Universal Declaration of Human Rights (UDHR) and other international human rights treaties provide a foundation for human-rights theory, various scholars have asserted that technological innovations, in all the epochs of industrial revolutions, have also affected international law, and by extension human rights.²⁵

3 IMPACT OF TECHNOLOGY ON DEVELOPMENT OF HUMAN RIGHTS

Compared to ancient international law, contemporary international law is inextricably linked to ever-unfolding technological developments. The emergence of the age of information technology and its influences on international law and human rights in particular make the current period more interesting. The increased interest in human rights in this field can be ascribed, in the main, to developments in international space law and to the international regulation of weapons of mass destruction.

Advancements in ship and navigation technologies resulted in the first waves of globalisation in the world's economy, thus enhancing diplomatic relations among nations and their behaviour towards each other. For instance, during the Spanish *conquistadores*, navigational aids were used in the oceans resulting in the "discovery" (according to a Eurocentric view) of native peoples, especially in the Americas.²⁶

The production and proliferation of new military technologies, such as gunpowder in 1648, contributed immensely to the development of international law and later ushered in the Treaty of Westphalia. The treaty was regarded as the foundation of the modern international order as it resulted in the acknowledgement of the coexistence of sovereign states. It must be noted that the same military technologies and weaponry were used during the First World War, while nuclear armaments played a key role in the Second World War. Following these two developments, the Permanent Court of International Justice was established and, later, the United Nations Organisation came into being. The subsequent manufacture of new technology-enhanced weaponry led to the generation of landmark legal innovations to mitigate threats to international peace.

²⁴ Prabhakaran, Mitchell, Gebru and Gabriel "A Human Rights-Based Approach to Responsible AI" 2022 *arXiv:2210.02667*.

²⁵ Maas "International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order" 2019 20(1) *Melbourne Journal of International Law* 29–56.

²⁶ Merrills "Francisco De Vitoria and The Spanish Conquest of the New World" *The Irish Jurist* 1968 3(1) 187–94 <http://www.jstor.org/stable/44026069> (accessed 2023-07-08).

From the 1950s to the 1970s, the outer space law, the law of the sea and international law continued to develop and dominate, especially in relation to the testing of nuclear weapons and energy. As a result, information technologies, the Internet and AI are now the technologies that have a historical connection with emerging human rights law. It is important to indicate that the private sector has, throughout, been complicit and highly involved in influencing the development of the international law regime, as Ohlson asserted.²⁷ This is because within the private sector exist various interests and ambitions with different (including transnational global) agendas. As a result, different versions of how technology can be useful are fed to government officials and bureaucrats in order to influence policy direction and the make-up of envisaged legislative frameworks to the advantage of those having an upper hand. In some instances, government officials are misled, hoodwinked or lured by massive kickbacks.

In the case of *Irma Flaquer*, the Inter-American Commission on Human Rights received a petition comprising complaints involving numerous human rights violations, including breaches of media freedom and access to information, kidnapping and the murder of a journalist in Guatemala.²⁸ The petitioners alleged that the journalist was a victim of forced disappearance and had been presumably murdered owing to their revelation of massive corruption involving senior government officials, the military and multinational companies. As part of a compromise to end countrywide protests and pressure from civil society, the Guatemalan government transformed its media laws into a settlement that was made an order of the regional body.

In South Africa, the Constitutional Court, in *Glenister* held:

“Endemic corruption threatens the injunction that government must be accountable, responsive and open. ... It is incontestable that corruption undermines the rights in the Bill of Rights and imperils democracy.”²⁹

4 THE ROLE OF SOFT LAW IN THE DEVELOPMENT AND GOVERNANCE OF AI SYSTEMS

Soft law can be defined as comprising those international norms, rules and principles that guide states and international non-state parties in their relations with no binding effect. Soft law operates where there is no degree of normative content to create enforceable rights and obligations.³⁰ Although it may have certain legal effects, it is nevertheless not binding. In the absence of binding legal norms, soft law serves to close the unregulated gap, guiding states and other stakeholders in the right direction. In the absence of a clear legislative instrument regulating the recognition and

²⁷ Olson "Corporate Complicity in Human Rights Violations Under International Criminal Law" 2015 1(3) *International Human Rights Law Journal* <https://via.library.depaul.edu/ihrli/vol1/iss1/5> (accessed 2023-06-30).

²⁸ *Irma Flaquer v Guatemala*, Case 11 766 Report No 67/03 Inter-Am CHR OEA/Ser LV/II 118 Doc 70 rev 2 at 635 (2003).

²⁹ *Glenister v President of the Republic of South Africa* [2011] ZACC 6 par 176 and 177.

³⁰ Choudhury "Balancing Soft and Hard Law for Business and Human Rights" 2018 67(4) *International & Comparative Law Quarterly* 961–986.

governance of AI systems at the international level, a credible body of soft-law rules has been established, at least informally at regional and national levels. The abrupt surge of the coronavirus pandemic in early 2020 spurred many jurisdictions into legislating and regulating various aspects of societal life so as to contain and control the disease. Some of these measures were seen as draconian as they interfered with some fundamental rights. Various organs of the UN also issued regulations and policy guidelines as part of disease management.³¹ In contrast, the international community has not applied the same energy and zeal to tackling the emergence of AI in the era of the 4IR.

Some scholars argue that self-regulation of AI systems by corporate companies should be left to unfold because it may work to the advantage of humanity.³² The disadvantage of such an approach is that humanity might lose the only opportunity available to assert itself over AI before it surpasses human intelligence.³³ On the other hand, subjecting AI to hard laws could be negative because it may scupper creativity and ultimately the potential for the full development of AI. Both the public and private sectors have been actively involved in the development of a body of soft-law rules that attempt to regulate AI, at least at the operational level.³⁴ This partnership has gone to great lengths, such that an implied consensus has been reached on the basic management and governance of AI systems. While there is laxity in some instances, various agreements and conventions have been adopted and complied with. Most such agreements are based on and guided by important international instruments such as the Universal Declaration of Human Rights.

To establish some regulatory framework, various states and stakeholders have committed themselves to using the advantages of AI and to minimising possible inherent risks. To this end, states and regional bodies, together with the private sector, have adopted some agreements and treaties. In the EU, states have agreed to adopt the Ethics Guidelines for Trustworthy Artificial Intelligence,³⁵ as well as the Assessment List for Trustworthy AI.³⁶ The Guidelines identified key principles and requirements for trustworthy AI,

³¹ The United Nations, through the World Health Organisation, went to great lengths to ensure that the disease was mitigated and controlled. Some of the guidelines and policy directives are found at <https://www.ohchr.org/en/covid-19/covid-19-guidance> (accessed 2022-06-29).

³² Candelson, Di Carlo, De Bondt and Evgeniou *AI Regulation Is Coming* 2021 99(5) *Harvard Business Review* <https://hbr.org/2021/09/ai-regulation-is-coming> (accessed 2023-07-04).

³³ Snider "Evolving Online Terrain in an Inert Legal Landscape: How Algorithms and AI Necessitate an Amendment of Section 230 of the Communications Decency Act" 2022 107 *Minn L Rev* 1829.

³⁴ Blanchette and Tolley *Public and Private Sector Involvement in Healthcare Systems: A Comparison of OECD Countries* (May 1997, revised February 2001) <https://publications.gc.ca/Collection-R/LoPBdP/BP/bp438-e.htm> (accessed 2023-07-07).

³⁵ European Commission "Ethics Guidelines for Trustworthy AI" (April 2019) [https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai#:~:text=According%20to%20the%20Guidelines,%20trustworthy%20AI%20should%20be:%20\(1\)%20lawful](https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai#:~:text=According%20to%20the%20Guidelines,%20trustworthy%20AI%20should%20be:%20(1)%20lawful) (accessed 2024-09-30).

³⁶ European Commission "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment" (17 July 2020) <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment#:~:text=The%20Ethics%20Guidelines%20introduced%20the%20concept%20of%20Trustworthy%20AI,%20based> (accessed 2024-09-30).

while the Assessment List provides a framework to support compliance with ethical standards by developers and users of AI. The Guidelines also address issues of data protection, algorithmic transparency, and openness, among other issues. The General Data Protection Regulation (GDPR) is regarded as the centrepiece of the EU law that regulates automated processing of personal data in the European Economic Area.³⁷ The regulations play a key role in safeguarding the fundamental rights that are threatened by the deployment and use of AI systems and related technologies. The Treaty on the Functioning of the European Union adds impetus by laying down principles of non-discrimination as a fundamental value, especially in articles 2 and 10, which require the EU to combat discrimination on listed grounds.³⁸ The European Union Charter on Fundamental Rights serves as a primary regional instrument and directly and indirectly provides a basis for the regulation of AI systems.³⁹ This can be seen in articles 20 and 21, which provide for equality before the law and non-discrimination. Such values are further elucidated in a raft of non-discrimination directives, with varying scopes of application that enshrine more detailed sector-specific legislation and directives aimed at safeguarding fundamental human rights.⁴⁰ In the EU, the Council of Europe's ad hoc committee on AI (CAHAI) is considering a proposal for an AI treaty and a pilot study to this effect has already been put in place. The proposals for the AI treaty contain key values, mostly derived from the OECD's five Principles on AI.⁴¹ The principles include the following:⁴²

"AI should benefit people and the planet by driving inclusive growth, sustainable development, and human well-being. AI systems should be designed in a way that respects the rule of law, human rights, democratic values, and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society. There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them. AI systems must function in a robust, secure, and safe way throughout their life cycles and potential risks should be continually assessed and managed. Organisations and individuals developing, deploying, or operating AI systems should be held accountable for their proper functioning in line with the above principles."

³⁷ The EU's General Data Protection Regulation was adopted in 2018 by the EU as part of harmonising data privacy laws across Europe. "General Data Protection Regulation (GDPR)" (undated) <https://gdpr-info.eu/> (accessed 2024-09-30).

³⁸ The Treaty on the Functioning of the European Union (TFEU), was developed in 2007 from the Treaty establishing the European Community (TEC or EC Treaty), which sought to establish the European Economic Community (TEEC), signed in Rome on 25 March 1957.

³⁹ The Charter of Fundamental Rights of the European Union came into force in 2009 and is intended to bring together the most important personal freedoms and rights enjoyed by citizens of the EU into one legally binding document.

⁴⁰ These include Employment Equality Directive (2000/78/EC), Racial Equality Directive (2000/43/EC), Gender Goods and Services Directive (2004/113/EC), and the recast Gender Equality Directive (2006/54/EC). In addition, the majority of EU member states are also party to other international human-rights conventions.

⁴¹ In May 2019, the OECD AI Principles were adopted by 40 countries in the West to promote innovation and trustworthiness in terms of human rights and democratic values by setting standards that are practical and flexible enough to stand the test of time. The OECD Artificial Intelligence (AI) Principles – <https://oecd.ai> (accessed 2022-07-03).

⁴² OECD. AI Policy Observatory "OECD AI Principles Overview" <https://oecd.ai/en/ai-principles/> (accessed 2022-07-03).

Currently, at the international level, sufficient soft-law rules have been developed and entrenched to cope with the deployment and use of AI systems globally. While the rules are not binding, some possess some degree of enforceability and are compulsory.

5 EMERGING FUNDAMENTAL RIGHTS

AI may change international legal situations by enabling new behaviours and by generating new legal entities.⁴³ In the same way, it may also change how states interact with international law, which may also have ramifications for human rights. In her theory of law and technology, Moses argues that technology creates recurring dilemmas for law, as it contributes to the formation of new entities and new behaviours.⁴⁴ These observations imply that there is a need for the development of *sui generis* rules to handle newly created technological situations and behaviours. Among others, the behaviours may include the systematic monitoring and control of populations through enhanced surveillance technologies, which have negative impacts on existing human rights such as privacy and dignity.

The impact of newly created legal behaviours and situations may also result in legal uncertainty and conflicting rules, since existing laws may not be adequate to cope with the classification of new activities, relationships and entities. According to Scherer, technological challenges posed by these situations are a result of the autonomy, opacity and unpredictability of certain AI systems, leading to uncertainty on issues of attribution, control and responsibility.⁴⁵

In enacting new legislative frameworks to cater for new technological challenges, the possibility exists that their scope may be incorrect resulting in over-inclusiveness or under-inclusiveness.⁴⁶ This may be the case where liability is to be determined for new technological entities powered by AI operating on their own, without human involvement. A case in point would be the incorporation of a limited liability company whose memorandum of incorporation may place it under an AI system.⁴⁷ An additional challenge may be that existing laws are rendered obsolete as they may no longer be justified, needed or cost-effective owing to the production and deployment of AI systems. On how technology may render *jus in bello* principles regulating international humanitarian law obsolete, Mandel argues that this could be the case where AI-powered combat platforms are deployed on the battlefield, replacing human soldiers, and thus throwing to the fore questions

⁴³ Maas 2019 *Melbourne Journal of International Law* 29–57.

⁴⁴ Moses “Why Have a Theory of Law and Technological Change?” 2007 8 *Minn JL Sci & Tech* 589 <https://scholarship.law.umn.edu/mjlst/vol8/iss2/12> (accessed 2023-07-05).

⁴⁵ Scherer “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies” 2015 29(2) *Harvard Journal of Law & Technology* <https://ssrn.com/abstract=2609777> (accessed 2022-07-05).

⁴⁶ McAllister “Stranger Than Science Fiction: The Rise of AI Interrogation in the Dawn of Autonomous Robots and the Need for an Additional Protocol to the UN Convention Against Torture” 2016 101 *Minn L Rev* 2527.

⁴⁷ Bayern “The Implications of Modern Business Entity Law for the Regulation of Autonomous Systems” 2015 19 *STAN TECH L REV* 93 https://law.stanford.edu/wp-content/uploads/2017/11/19-1-4-bayern-final_0.pdf (accessed 2023-07-05).

on how humanitarian-law principles affect the treatment of prisoners of war in such a scenario.⁴⁸

6 IMPACT OF TECHNOLOGY ON SELECTED VULNERABLE HUMAN RIGHTS

The UDHR serves as the source from which human and fundamental rights are derived and have evolved over time. It remains a source for all these rights and has informed subsequent binding and non-binding international, regional and national instruments regulating human and fundamental rights. Key instruments, among others, include the International Covenant on Civil and Political Rights (ICCPR),⁴⁹ the European Convention of Human Rights and the African Charter.⁵⁰

In South Africa, human and fundamental rights are contained in Chapter 2 of the Constitution of the Republic of South Africa, 1996 (Constitution) and in related legislation.⁵¹ The transformative nature of the Constitution is evident in section 8(3), which provides that in interpreting the Bill of Rights,⁵² the courts must develop rules and the common law to give effect to a constitutional right, and may also limit a right with the proviso that a limitation is in accordance with the provisions of section 36(1). Similarly, the interpretation clause in section 39(2) provides for courts and related bodies to consider international and foreign law when interpreting any legislation, and to promote the spirit, purpose and object of the Bill of Rights. Section 39(3) is interesting in that it accommodates any other rights conferred by common law, customary law or legislation, provided they are in line with the overall provisions of the Constitution.⁵³ According to Klare, a post-liberal approach is the best way to interpret the Bill of Rights in South Africa,⁵⁴ informed (among other things) by the consciousness of key aspects of transformative constitutionalism such as social rights, substantive equality, multiculturalism, participatory governance and consistent fulfilment of positive obligations by the State. This means that courts must not be trapped

⁴⁸ Mandel "Legal Evolution in Response to Technological Change" in Brownsword, Scotford and Yeung (eds) *The Oxford Handbook of Law, Regulation, and Technology* (2017) 225-233-4.

⁴⁹ The ICCPR, which was adopted on 16 December 1966 and initially signed by 116 States Parties, is currently ratified by 117 of the 193 UN member states. South Africa and a significant number of EU member states are also parties to the Covenant.

⁵⁰ The European Convention on Human Rights was adopted by the Council of Europe in 1950 and entered into force on 3 September 1953. Similarly, the African Charter on Human and Peoples Rights came into being in 1981 and entered into force in 1986. In the main, the two instruments are designed to promote human rights.

⁵¹ The European Convention of Human Rights came into force on 3 September 1953 and was acceded to by all the 27 member states in the EU.

⁵² S 8(3) imposes a duty on the courts to apply and develop common-law rules, subject to the limitation clause contained in s 36(1), while s 8(2) provides that the Bill of Rights applies and binds a natural or a juristic person, depending on the nature of the right and nature of the duty imposed by that right.

⁵³ Section 39(3) provides that "the Bill of Rights does not deny the existence of any other right or freedoms that are recognised or conferred by common law, customary law, or legislation, to the extent that they are consistent with the Bill of Rights."

⁵⁴ Klare "Legal Culture and Transformative Constitutionalism" 1998 *South African Journal on Human Rights* 153-154 [10.1080/02587203.1998.11834974](https://doi.org/10.1080/02587203.1998.11834974) (accessed 2022-12-20).

in classical notions of human rights when interpreting constitutional provisions but must instead adopt transformative constitutionalism. Allison concurs with Klare that the Constitution places positive duties on the State to create a more egalitarian and equal society, rather than simply protect liberties as in a classical liberal design.⁵⁵

New technological developments, in the form of the Internet of Things, AI, 3D technology and sophisticated algorithms, are, on the one hand, bound to have a significant impact on existing human and fundamental rights, and on the other, have the potential to give rise to new rights. Based on the discussions above, it is clear that most of these potential rights cannot be accommodated in existing legislative and regulatory frameworks. In South Africa, the right to Internet access has, at the time of writing, been curtailed for over 17 years as a result of delays by the telecoms regulator, the Independent Communications Authority of South Africa (ICASA), in allocating licences for radio-frequency spectrum for various uses. This has obstructed the realisation of much-needed low data costs and increased network capacity provided by the rollout of 4G and 5G technologies for high-speed broadband. The radio-frequency spectrum is a limited natural resource used to carry information wirelessly; it is vital and critical for social life as it enables telecommunication, radio broadcasting, television, cellular phones and the Internet through the transmission of electronic signals. Therefore, free availability and unfettered access to the frequency spectrum have implications for a myriad of constitutional values and rights, such as freedom of trade and freedom of expression and information, including universal access to the Internet. Radio-frequency spectrum is allocated through undersea cable by the International Telecommunications Union, of which South Africa is a member, while locally, it is allocated by the Minister of Telecommunications in the radio-frequency plan.

Control of the radio-frequency spectrum in South Africa is vested with ICASA in terms of section 30(1) of the Electronic Communications Act and the related legislative framework.⁵⁶ The regulator controls, plans, manages and administers the use and licensing of radio-frequency spectrum,⁵⁷ in line with the National Radio Frequency Plan 2018, which has been prepared under section 34 of the Act.⁵⁸ The impact of these technologies can be seen in three ways: the violation of rights; potentially conflicting rights; and new

⁵⁵ Klare 1998 *South African Journal on Human Rights* 154.

⁵⁶ Electronic Communications Act 36 of 2005. It should be noted that the two statutes that regulate the use of radio frequency, i.e., the Independent Communications Authority Act 13 of 2000 (the ICASA Act), and the Electronic Communications Act 36 of 2005 (ECA) were each amended recently by the Electronic Communications Amendment Act 1 of 2014. Together, they are the statutory foundation for the regulatory regime for radio-frequency spectrum.

⁵⁷ S 2 of the ICASA Act describes ICASA as an independent authority, mandated to regulate electronic communications in the public interest. In terms of section 3(3), it is further expected to act independently and subject only to the Constitution and the law, meaning that ICASA must be impartial in performing its functions without fear, favour or prejudice. In carrying out this mandate, ICASA is obliged to comply with both bilateral agreements and international treaties entered into by the Republic.

⁵⁸ ICASA "National Radio Frequency Plan 2018 (NRFP-18)" GN 266 in GG 41650 of 2018-05-25 https://www.gov.za/sites/default/files/gcis_document/201805/41650gen266.pdf (accessed 2023-07-14).

issues emanating from the use of new technologies. A violation of rights may arise, for example, when AI analytics systems interfere with privacy rights, or when risk profiling discriminates against any individual. Conflicting rights may arise in instances that use AI systems for intelligence gathering in the interest of public safety and the opposing right to privacy. New issues would include the right to anonymity, to oblivion or to not be forgotten, as provided for in article 17 of the EU's GDPR.

The contemporary regulatory landscape for AI systems attempts to address their undesirable impact, while also striving to enhance innovation and technology development. There is a degree of legal uncertainty as to how existing legislative and regulatory frameworks can address both the violation of existing rights and conflicting rights. This leaves citizens exposed to potential violations with no or few legal protections. Existing human and fundamental rights were conceived and drafted many years ago,⁵⁹ and were formulated in general terms that align with ethical and societal values, as opposed to specific current situations and environments. While existing rights were widely phrased to provide sufficient space for interpretation and application, the values underpinning these rights have fundamentally evolved and changed.⁶⁰ This is attested to by Custers, who argues that the rise of social media platforms has resulted in people increasingly sharing personal information, thus diluting perceptions regarding the right to privacy, for instance. This demonstrates not only regulatory gaps in privacy rights but also applies to many other fundamental and human rights threatened by the deployment and use of AI systems.

In order to identify these gaps, Custers argues that the assessment of how these rights apply in practice may result in stretching the interpretation of existing legal frameworks and possibly yielding untenable distortions that drift away from how the rights were originally conceived, leading to legal uncertainty.⁶¹ To address this, the EU adopted the Declaration on European Digital Rights and Principles for the Digital Decade in December 2022, as a commitment to safe, secure and sustainable digital transformation that prioritises European people, underpinned by European core values and principles. The principles are shaped around six themes:

“They include putting people and their rights at the centre of the digital transformation, supporting solidarity and inclusion, ensuring freedom of choice online, fostering participation in the digital public space, increasing safety, security and empowerment of individuals and promoting the sustainability of the digital future.”⁶²

⁵⁹ For instance, the European Convention on Human Rights (ECHR) and the GDPR were adopted and ratified in the 1950s when there was no Internet or AI systems.

⁶⁰ Custers “New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era” 2022 44 *Computer Law & Security Review* <https://www.sciencedirect.com/science/article/pii/S0267364921001096> (accessed 2023-03-09).

⁶¹ Custers 2022 *Computer Law & Security Review* 5.

⁶² The European Declaration on Digital Rights and Principles for the Digital Decade was adopted in December 2022 and serves as a vision for digital transformation, in line with EU values and fundamental rights. The Declaration provides a reference framework for citizens and guides the EU and Member States on a digital transformation journey. European Commission “European Declaration on Digital Rights and Principles for the Digital Decade” (15 December 2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> (accessed 2023-03-07).

To assess this Declaration and the digital rights it proposes, the article discusses specific digital rights identified in the literature across the board.

6.1 Privacy rights and data protection

The development, as well as the training, testing and use of AI systems that rely on the processing of personal data, is supposed to secure and respect personal privacy rights fully. These privacy rights also relate to a person's family life and the right to self-determination in relation to their data. Privacy rights are protected under article 12 of the UDHR and article 17 of the ICCPR, which affords a person protection of individual privacy rights in their home, including their correspondence as well as personal honour and reputation. These rights are further explicitly enshrined in article 8 of the EU's Charter of Fundamental Rights, which guarantees the protection of the right to personal data.⁶³ The provisions further require consent as a precondition before personal data can be fairly processed for a legitimate purpose. In this way, privacy is viewed as a fundamental right that is essential to human security and comfort. The right is also interwoven with other rights, such as the right to freedom of expression and association. It is also closely related to the right to privacy and as a result, it can be considered to be part of the UN human-rights system. It is for this reason that most governments in the EU now recognise the right to data protection.

Article 50 of the draft EU AI Act and its Regulations imposes certain transparency obligations for corporate companies.⁶⁴ These obligations include that a person must be informed when their character or emotions interact with an AI system, such as a chatbot. Such an obligation also arises where there is a manipulation of image, audio or video content by an AI system through automation, though there are exceptions to this case. Most significantly, AI systems are trained to use analysis of big datasets to provide feedback through the collection, refinement, and calibration of personal data. It is during these processes that sensitive personal and private information about individuals is collected and stored. Some of these models are able accurately to estimate personal data by merely using previous and future locations of cell phones, including those of a person's close associates.⁶⁵ It is clear that most such personal details are protected information that must be treated with all sensitivity and respect for the person concerned.

⁶³ Article 8 provides that: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

⁶⁴ The draft EU AI Act has been in place for consultations and was expected to be passed into law in subsequent months.

⁶⁵ Bellovin and Hutchins "When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning" 2014 8(2) *NYU Journal of Law and Liberty* 555-628 https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2379&context=fac_pubs (accessed 2022-08-25).

In the EU, the European Court on Human Rights, in the *Liberty* case,⁶⁶ dealt with the requirement of foreseeability when surveillance measures are used in the interception of communication. The surveillance measures were used to monitor a person through filtering techniques. The techniques consisted of automated sorting systems that selected keywords from a technical database.⁶⁷ In this case, the court ruled that the applicable law at the relevant time did not indicate, with sufficient clarity, adequate protection against abuse of power by the State regarding the interception and examination of external communications.⁶⁸ The reason for this insufficiency relates to fragmented legislation in the EU on this aspect. The current proposals seek to harmonise regulations within the EU. As a result, the court found that the existing law does not spell out the procedure for selection, examination, sharing and storing of data intercepted from individuals. Accordingly, it was ruled that the interference with the applicants' rights could not be regarded as violating article 8 of the ECHR.

Among other things, notification to concerned individuals should always be at the fore, although it should not necessarily take place during surveillance, but afterward so as not to defeat the object of surveillance. Therefore, the court in *Liberty* viewed notification as being inextricably linked to safeguarding against abuse of surveillance measures that are intrusive to privacy rights.⁶⁹

6.2 Vulnerable platform workers and the right to work

States Parties are obliged to work towards the full realisation of the right to work and adequate living standards in line with the provisions of articles 6 and 11 of the International Convention on Economic, Social and Cultural Rights (ICESCR).⁷⁰ There is a recognition by the parties that appropriate steps must be taken to ensure that everyone is granted an opportunity to earn their living to fulfil these rights. While these rights are not absolute, States Parties are obliged to work towards achieving these rights as they constitute the minimum core obligations within the UN human rights system.

The deployment of AI systems at the workplace poses a serious challenge to the constitutionally protected right to work, especially to vulnerable platform workers whose rights are violated and who face discrimination. One of the most visible and disconcerting effects of the latest technological revolution in the world of work is represented by digital labour platforms. These platforms bear different names and business models, and play different roles, vacillating between labour brokers, outsourcing and

⁶⁶ *Liberty v the United Kingdom* (58243/00) ECHR 01/07/2008 <https://hudoc.echr.coe.int/eng#{%22itemid%22:%22001-87207%22}> (accessed 2022-08-25).

⁶⁷ *Liberty v the United Kingdom supra* 43.

⁶⁸ *Liberty v the United Kingdom supra* 69.

⁶⁹ *Liberty v the United Kingdom supra* 67.

⁷⁰ Article 6 requires State Parties to recognise the right to work, which includes the right to choose or accept work that provides a living, while Article 11 urges State Parties to recognise the right to an adequate standard of living, including food, clothing, and housing amongst others.

intermediaries based on labour demand and supply. Most affected workers only interact or work from home, or work as telemarketers for various apps and platforms that are AI-driven. According to Rasioru, this has become a common practice in Romania where different digital platforms and apps circumvent existing labour laws to manipulate desperate workers.⁷¹

Most public sector entities and companies procure AI systems from specialist tech companies for purposes that include advertisement, recruitment, performance management and payroll management systems. Machine-learning algorithms used by these third-party companies may reinforce human prejudices targeting unsuspecting employees. For example, unscrupulous advertising companies may use algorithms to target people with low incomes to generate high-interest loans. The reality of the matter internationally is that existing employment laws are crafted and geared at preventing discrimination based on the grounds of race, sex, religion, disability and age, among other grounds. In evaluating individual employees for possible employment or promotion, AI systems are used to choose suitable candidates, and it may prejudice anyone based on these particular grounds. A real threat exists that automation of jobs by AI could result in massive job losses and unemployment, resulting in an infringement of the right to work and, ultimately, of the right to adequate living standards. Throughout the world, the automation of workplace operations has already resulted in the shedding of jobs in certain economic sectors. It would seem that this trend will continue to rise with time. Conversely, there is consensus that effective use of AI will also yield more jobs as opposed to job destruction, given expected shifts in the labour market.

The use of software for background screening has also raised concerns, not only regarding the possible perpetuation of discriminatory practices against potential employees but also with regard to organisational rights at the workplace. The emergence of the novel coronavirus forced many companies to fall back on home-based remote working, using technological tools of the trade linked to company servers. This has resulted in significant union bashing and has limited employees' right to assemble, protest and bargain, especially with regard to employees' loss of benefits as a result of lockdown regulations throughout the world.⁷² In the midst of this, the data protection authorities declared invalid the use of fingerprints at the workplace as part of the clocking system in Italy⁷³ and Greece.⁷⁴ This was because such mechanisms use AI systems that infringe on the right to privacy, dignity and personal data. The basis of these decisions is that the purpose of using

⁷¹ Rosioru "The Status of Platform Workers in Romania" 2020 41 *Comp Lab L & Pol'y J* 423 <https://heinonline.org/HOL/P?h=hein.journals/cllpj41&i=447> (accessed 2022-06-29).

⁷² Major international brands such as H&M, Michael Kors, Zara and Levi Strauss have been accused of union busting and unfairly dismissing or suspending workers during the Covid-19 lockdown in countries like Myanmar, Bangladesh and Cambodia. The rationale for this was solely to reduce their production costs, while workers would be in a weaker position. See Business and Human Rights Resource Centre "Union Busting and Unfair Dismissals: Garment Workers During COVID 19" https://media.business-humanrights.org/media/documents/files/200805_Union_busting_unfair_dismissals_garment_workers_during_COVID19.pdf (accessed 2022-09-28).

⁷³ The Garante per la protezione dei dati personali, Provision of July 21, 2005.

⁷⁴ The Greek Data Protection Authority, Decision of 20/3/2000.

fingerprints could still be attained using other systems that do not impinge on privacy and do not involve an employee's body.

The use of AI systems may also affect the right to work, especially for workers whose responsibilities include driving any connected and automated transport. In the EU, liability for connected and autonomous driving is currently regulated at both the Union and national levels by adopting different approaches. On the one hand, they use norms regulating the fault-based liability of the driver, and on the other the objective liability of the owner, coupled with the European product-liability regime.

Germany is one of the first EU states formally to adopt a legal framework for allowing the user of a vehicle to disengage from driving completely.⁷⁵ The legislation also imposes a ban on non-passenger driving systems, except for low-speed parking systems operating on private property.⁷⁶ The legislation further prescribes that the design of these vehicles should allow for proper space and time to transition from an automated system to a human-driver system to ensure there is control. It is also obligatory for manufacturers to install electronic units and black boxes in vehicles; these are mainly used for recording the operations of connected and autonomous driving. According to the legislation, if a driver is at fault, they will be held liable; if not, the owner is held accountable for damages. The owner may still sue the manufacturer in claims for product liability.

6.3 The right to Internet access or to be online

Internet access has become critical in the 4IR as most services and products are only offered online, sometimes reasonably cheaply, but may be expensive if purchased offline. Inability or obstacles to accessing the Internet put people in a disadvantageous position, especially when it comes to public-service job applications, access to social services and submission of online tax returns. Similarly, some repressive regimes have resorted to shutting down the Internet in order to stamp authority over civilian protests and uprisings.⁷⁷ To ensure access to applications for social-relief grants, the South African government used electronic systems in 2020 during the COVID-19 state of disaster. Most applicants found it difficult to submit their applications online owing to a lack of free access to the Internet. According

⁷⁵ The Law of 11 June 2017, the Federal Law Gazette, Amending the Road Traffic Act, as announced on 5 March 2003 (Federal Law Gazette 310). Gesley "Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads" 2021 <https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/> (accessed 2022-06-30).

⁷⁶ Bertolini and Riccaboni "Grounding the Case for a European Approach to the Regulation of Automated Driving: The Technology-Selection Effect of Liability Rules" 2021 51 *European Journal of Law and Economics* 243–284 <https://link.springer.com/article/10.1007/s10657-020-09671-5> (accessed 2022-06-30).

⁷⁷ Report of the Office of the United Nations High Commissioner for Human Rights: Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights, (13 May 2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/55/PDF/G2234155.pdf?OpenElement> (accessed 2023-03-08).

to the collaborative study by the National Income Dynamic Study, the applications systems collapsed and this delayed payment of such grants.⁷⁸

Section 2 of the ICASA Act describes ICASA as an “independent authority”, mandated to regulate electronic communications in the public interest; and in terms of section 3(3), it is expected to act independently, “subject only to the Constitution and the law, and must be impartial and must perform its functions without fear, favour or prejudice”. In carrying out this mandate, ICASA is obliged to comply with bilateral agreements, as well as international treaties entered into by the Republic. These provisions were the subject of protracted legal tussles between the Minister, ICASA and service providers in the telecommunications industry; among other things, the delays denied a basic right of access to the Internet.⁷⁹ The bone of contention in this case centred on the independence and extent to which ICASA as a regulator and a Chapter 9 institution can exercise its discretion in the allocation of radio-frequency spectrum. The issue was whether ICASA is legally entitled to issue an Invitation to Apply (ITA) for auctioning rights to use certain bands of radio-frequency spectrum to mobile and non-mobile operators, without considering ministerial policy or the White Paper. It was alleged that the ITA did not comply with the radio-frequency plan and statutory obligations aimed at promoting competition.⁸⁰ The Minister approached the court to set aside this decision by ICASA. The radio-frequency plan in force was drafted by ICASA and approved by the Minister in order to regulate the allocation of various uses of spectra in mobile telecommunication and broadcasting, with ranges of 700mhz, 800mhz and 2.6ghz bandwidth.⁸¹ The Minister argued that the bandwidth in issue cannot be made available for exclusive use by mobile networks under the plan and that the plan would have to be amended to provide for exclusive use. It was further argued that exclusive assignment to mobile operators cannot take place until non-mobile operators are migrated from the above bandwidth, hence their unavailability.⁸²

In turn, the counter-argument by ICASA was that the radio-frequency plan does allow for multiple uses and that it is empowered by sections 31(3) and (4) of the Electronic Communications Act⁸³ to migrate operators out of a spectrum by changing the terms of the licence. It was held that although a conditional assignment would not adversely impact non-mobile operators who had already been assigned spectrum, it would be invalid to re-assign the spectrum to mobile operators. Regarding the interpretation of the radio-spectrum plan and its enabling legislation as to whether the allocation by the Minister could precede the assignment of licences by ICASA for exclusive use by mobile operators for only eligible usages, it was held that the contemplated assignment by ICASA would “be out of kilter with the

⁷⁸ Wills “Household Resource Flows and Food Poverty During South Africa’s Lockdown, Short-Term Policy Implications for Three Channels of Social Protection” 2023 https://www.uj.ac.za/wp-content/uploads/2021/10/nids_cram-wave-1.pdf (accessed 2023-03-08).

⁷⁹ *Minister of Telecommunications and Postal Services v Acting Chair, Independent Communications Authority of South Africa* [2016] AGPPHC 883.

⁸⁰ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 18.

⁸¹ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 50.

⁸² *Minister of Telecommunications & Postal Services v Acting Chair supra* par 51.

⁸³ 36 of 2005.

prescribed ‘allocations’”.⁸⁴ Secondly, it was held that the envisaged deference of amendment of the plan by the Minister would be invalid and irrational.⁸⁵ However, the court had to consider exceptional circumstances posing possible irreparable harm and balance of convenience to respondent companies if an interdict were granted. The court observed thus:

“[T]he assignment of spectrum already assigned to other operators is of questionable validity and secondly, to assign now and defer access to an unknown future date, which is dependent on a host of process-dependent happenings has the look of a reckless decision and for that reason an irrational decision. In my view, there is a real prospect that the review court could reach these conclusions. A prima facie case is made out.”⁸⁶

Based on these observations, the court found that bidding by the respondent companies based on the ITA would incur substantial costs, running into millions of rands and that dismissing the application for an interdict ran the risk of violating the rule of law. The court was of the view that potential irreparable arising from substantial costs incurred by respondent companies would amount to exceptional circumstances justifying the granting of an interdict as per prayers.⁸⁷ It must also be indicated that article 19 of the UDHR points to a right to the Internet, in that it recognises the right to freedom of opinion and expression, as well as access to information.⁸⁸ In particular, to give effect to the right to the Internet, the UN Human Rights Council, in 2021, passed a resolution declaring that access to the Internet was a catalyst to the enjoyment of social, economic and cultural rights. However, the UN stopped short of recognising this particular right, and as such the resolution does not have binding force. It was adopted in anticipation of future technological developments.

The African Commission on Human and Peoples’ Rights adopted a Declaration of Principles on Freedom of Expression and Access to Information in Africa in 2002, later updated in 2019. The Declaration is geared at accommodating some of the novel but obscured digital rights occasioned by the 4IR.⁸⁹ It states: “[U]niversal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.” It may however be observed that conditions on the ground show that this principle is still far from realised. A precondition for access to the Internet is access to a stable power supply. According to the World Bank, only 46,5 percent of the population in sub-Saharan Africa had access to electricity in 2019. The share of people using the Internet in Africa as a whole was 39,3 percent in 2020, compared to 62,9 percent in the rest of the world. On the

⁸⁴ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 58.

⁸⁵ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 59.

⁸⁶ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 59–60.

⁸⁷ *Minister of Telecommunications & Postal Services v Acting Chair supra* par 78–83.

⁸⁸ Article 19 provides everyone with the right to freedom of opinion and expression. This right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media, regardless of frontiers.

⁸⁹ African Commission on Human and Peoples’ Rights “Declaration of Principles on Freedom of Expression and Access to Information in Africa” 2002 <https://achpr.au.int/en/special-mechanisms-reports/declaration-principles-freedom-expression-2019> (accessed 2022-12-22).

continent, regional and national differences are extreme, with 59,5 percent of people in southern Africa having Internet access.⁹⁰

6 4 The right to be offline or to disconnect

The right to be offline or to disconnect, especially after working hours, is currently applicable within the context of employment law in some countries. The right presupposes that employees may not be contacted by employers or their representatives outside working hours and days through any form of communication. These include emails, telephone calls or any other form of communication. While this is considered to be in line with existing labour legislation, it is advisable that employers put in place acceptable policy guidelines in consultation with their employees. Apart from the employment perspective, the propagation of the right is also considered to have some social benefits, especially in dealing with issues of Internet addiction and its negative impacts on society. From a social point of view, it is clear that compulsive and excessive uncontrollable use of the Internet, especially social media, tends to cause considerable anxiety, affecting the mental health and well-being of individuals. Therefore, the right to be offline and disconnected is expected to set and enhance necessary standards and expectations to prevent addictions and help people become productive members of society.

6 5 The right to change your mind

It should be noted that some websites would seldom require a person to enter their personal details and their preferences of what they want to see or know about, directly or indirectly. In this way, one would be required to disclose individualised preferences, which are then captured by algorithms to determine the kind of information, products and services that can be offered to you by inference.⁹¹ In a review of Pariser's works, Samuels argues that this demonstrates that the digital empires behind the websites may use their innocuous ways to monitor consumer behaviour, conduct purchase correlation research and predictive marketing, among others.⁹² Correctly, Pariser has characterised this as filter bubbles, where you are stuck and bombarded with feedback loops of information.⁹³ As a result, every time a person visits a particular website, this kind of information is displayed.

A critical question is what happens when a person changes their mind and is, for example, no longer interested in certain items or other social activities.

⁹⁰ Bussiek "Digital Rights are Human Rights, An Introduction to the State of Affairs and Challenges in Africa" (April 2022) *Friedrich Ebert Stiftung* <https://library.fes.de/pdf-files/bueros/africa-media/19082-20220414.pdf> (accessed 2023-03-09).

⁹¹ Samuels "Review: The Filter Bubble: What the Internet is Hiding From You by Eli Pariser" 2012 8(2) *InterActions: UCLA Journal of Education and Information Studies* <http://dx.doi.org/10.5070/D482011835> or <https://escholarship.org/uc/item/8w7105jp> (accessed 2022-07-20).

⁹² Samuels 2012 *InterActions: UCLA Journal of Education and Information Studies* 92.

⁹³ Pariser *The Filter Bubble: What the Internet is Hiding From You* (2011) 294. https://hci.stanford.edu/courses/cs047n/readings/The_Filter_Bubble.pdf (accessed 2022-07-20).

Attempts to change settings may not be effective since algorithms may try to prevent this, leaving one stuck in filter bubbles and echo chambers owing to previous preferences and interests. While articles 18 and 19 of the UDHR, together with articles 9 and 10 of the ECHR, guarantee the fundamental right to freedom of thought and expression, the state of current technological developments demands renewed and stronger protections for these rights. Such protections would go a long way to reinforcing the right to change your mind, by putting more weight on values supporting informed consent, online freedom and personal development, among others.

6 6 The right to know the value of your personal data

While the provision of online services and products such as search engines and social media platforms are freely available at no financial cost, companies offering these services make a profit by collecting, leasing and trading personal data on their systems. People are duped into believing that accessing these platforms is free, while there is in fact no free lunch in this world.⁹⁴ From a financial and economic perspective, it would seem that there is no transparency in how such data is processed. It is entirely unclear how the value of personal data is weighed and measured. It is valid for consumers using these platforms to exercise their right to know the value of their data.⁹⁵ The application of privacy rights is not feasible and adequate to protect the commodification of personal data collected from search engines and social media platforms. It is thus important to regulate the value attached to personal data as a commodity and this should include pricing models, bodies responsible for determining pricing and how this should be enforced.

6 7 The right to a clean digital environment

The universal right to a clean environment that is not harmful to human health and well-being is codified in various international instruments and pieces of legislation across jurisdictions. The right imposes obligations on governments and the private sector to strive for a clean environment. The continued efforts to digitise the world and narrow the digital divide come with a massive expansion of digital technologies and related infrastructure. Deliberate efforts must be put in place to ensure that this does not cause exponential energy consumption, harmful environmental impact and e-waste across the supply chains within the digital corporate world. An example is the use of blockchain technologies, which tend to use or generate very large amounts of energy, which may put pressure on the environment.⁹⁶

⁹⁴ Malgieri and Custers "Pricing Privacy: The Right to Know the Value of Your Personal Data" 2017 *Computer Law & Security Review* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047257 (accessed 2023-03-10).

⁹⁵ Malgieri and Custers 2017 *Computer Law & Security Review* 4.

⁹⁶ De Vries "Bitcoin's Growing Energy Problem" 2018 2(5) *Joule* 801–805; Dittmar and Praktiknjo "Could Bitcoin Emissions Push Global Warming Above 2°C" 2019 *Nature Climate Change* 656–657.

According to Coalition for Digital Environmental Sustainability (CODES), the digitalisation process is crucial to achieving the UN's Sustainable Development Goals (SDGs) by 2030. To this end, an assessment by CODES in 2020 found that 70 per cent of 169 targets base-lining the world's sustainability goals can be positively influenced using digital technology applications.⁹⁷ Thus the development of artificial intelligence technologies could result in destruction of the natural ecosystem as a result of the need for energy-intensive computing power and data centres. To this end, Zhuk argues that their impact could cause cooling problems while electronic waste could be formed due to the need for their continuous and rapid improvement.⁹⁸ This implies that technologies dominated by AI systems will play an influential role in environmental sustainability. With digital traces everywhere, it could therefore be argued that data will be the pollution issue in the 4IR. Combined with other data, digital pollution may result in digital biases and noises when sucked into the aggregation of data analysis, resulting in pollution of the online ecosystem.

7 PERTINENT LEGAL ISSUES THAT MAY GIVE RISE TO HUMAN RIGHTS VIOLATIONS

7.1 Transparency and explainability challenges

The possibility exists that the inner workings and interactions between components of an AI system may be opaque and unexplainable. Similarly, the involvement of multiple individuals and firms in the design, modification and incorporation of the components of AI systems may make it difficult to point to the exact party who is to be held responsible for any harm that may occur. It is highly possible that some components may have been designed a long time previously and also that a designer may not have foreseen that their designs would be used and incorporated into an AI system that would cause harm. With AI systems, anyone with access to modern smartphones and computer software can compose a computer code from anywhere in the world without needing the privileges of a resourceful large corporation.

7.2 Liability and accountability constraints

Despite well-established product-liability regimes in both South Africa and the EU, legal difficulties have arisen with software and hardware infrastructure insofar as AI liability is concerned. Another difficulty centres on whether software falls within the notion of a "product". One of the requirements for product liability is its characterisation of a product as a tangible thing. While software and hardware may originate from different companies, software components integrated into hardware are deemed to

⁹⁷ Koroleva "Action Plan for a Sustainable Planet in the Digital Age" (31 May 2022) https://wedocs.unep.org/bitstream/handle/20.500.11822/38482/CODES_ActionPlan.pdf?sequence=3&isAllowed=y (accessed 2023-03-10).

⁹⁸ Zhuk "Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues" 2023 1(4) *Journal of Digital Technologies and Law* 932–954 <https://doi.org/10.21202/jdtl.2023.40>.

be a product. Therefore, consideration of software as a product affects the liability of a software manufacturer together with a hardware manufacturer. On its own, software would qualify as a product if it were stored on a tangible medium like a DVD or memory stick. Confusion creeps in only when the software is downloaded, in which case no clarity exists as to how it should be treated in terms of the applicable product-liability regime.

Apart from autonomy, which encompasses foreseeability problems, AI systems also pose risks relating to control. Human control of machines that are programmed with considerable autonomy is bound to be difficult and may result in loss of control, malfunctioning, flawed programming, corrupted files, or damage to input equipment, among other problems. The possibility exists that when an AI system learns its environment and improves its performance, it may be difficult for humans to regain control once it is lost, and this may have catastrophic and existential risk consequences for humanity.⁹⁹ This depends on the ability of AI systems to improve their hardware and software programming to the extent of surpassing human consciousness and cognitive abilities.¹⁰⁰

7 3 Emergence and protection of new fundamental rights

While the international community, and the UN in particular, seems to have taken a backseat in actively agitating for the legal protection of vulnerable rights threatened by the emergence and deployment of AI systems, existing international instruments appear to withstand new threats to human and fundamental rights in the era of the 4IR. Emanating from the discussion above, it is observed that, on the one hand, new technologies are bound to have an adverse impact on existing human and fundamental rights, and on the other, they lay a solid base for the emergence of new rights. It is however clear that most of these potential rights cannot be accommodated in existing legislative and regulatory frameworks. The negative impact of these technologies can be identified in the form of the violation of rights, conflicting rights and new issues, all emanating from the use and deployment of new technologies.

Conflicting rights may also arise in instances where the interest of the public is at stake on the one hand, and when a corresponding right to privacy has to be protected on the other hand. The discussion finds that the interpretation and application of existing legal and regulatory frameworks may be overstretched and may yield untenable distortions that drift from how the rights were originally conceived, leading to legal uncertainty and possible infringement of legally protected rights.

⁹⁹ Akash "AI the Biggest Existential Threat to Humankind Says Elon Musk" (14 July 2021) *Analytics Insight* <https://www.analyticsinsight.net/artificial-intelligence/ai-the-biggest-existential-threat-to-humankind-says-elon-musk> (accessed 2023-01-18).

¹⁰⁰ Dr Roman Yampolskiy, a computer scientist from Louisville University, is of the view that "no version of human control over AI is achievable as it is not possible for the AI to both be autonomous and controlled by humans". Hamrud "AI Is Not Actually an Existential Threat to Humanity, Scientists Say" (11 April 2021) <https://www.sciencealert.com/here-s-why-ai-is-not-an-existential-threat-to-humanity> (accessed 2023-01-18).

7 4 Development and conceptualisation of relevant legislative frameworks

Responsible authorities at all levels should ensure that data collection processes are democratic, transparent and accountable with a view to eliminating any form of discrimination, biases and prejudice. There is a need to ensure that Internet connectivity is a basic commodity that is freely accessible, and provided to everyone. It has also been shown that a significant number of existing laws need to be revamped and adapted to conditions and environments for conducive deployment and operation of AI systems. This will ensure investor and business certainty in our laws, while also encouraging the responsible use of AI systems.

8 RECOMMENDATIONS

Having outlined various aspects of the impact of AI systems on human rights and noted how emerging pertinent rights could be affected, the following observations and recommendations have emerged. The recommendations are meant to serve as a guide to the development and shaping of rights arising from the use of AI systems.

It is clear that the radio-frequency spectrum is critical for access to reliable and cheaper Internet connection, and that delays in its roll-out are negatively affecting rights of access to the Internet and other connected rights. Both bureaucratic bungling and corporate selfishness have resulted in this situation. In this light, it is appropriate to recommend that both legislative and regulatory frameworks be reviewed to clarify the role of the regulator and the executive in relation to the allocation and assignment of the radio-frequency spectrum.

Since it is unfair to apportion blame to component designers whose work may be far removed in space and time from the completion and operation of AI systems, the conception of any regulation and legislation must try to ensure efficient disclosure of information, particularly where there are differences in time and geographic location between stakeholders involved in the development and production of AI systems.

In addition, regulation should ensure effective protection of the user's intellectual property, and encourage innovation in the deployment of AI systems in an equitable manner.

Given that the distinction between tangible and intangible objects becomes more blurred as we enter the 4IR, dominated by digital content, it is submitted that, in the medium to long term, a common-liability regime for AI systems should be developed to bring certain aspects of software into the product-liability fold.

It becomes imperative that the international community, led by the UN, should consider developing a specific international instrument focusing on various legal dimensions aimed at regulating AI systems and their implications for human and fundamental rights. The international community should also ensure that existing efforts to regulate international trade and copyright laws do not disadvantage developing countries. They must

therefore be aimed at ensuring equitable access to the benefits of AI systems since there should be a collective approach in confronting challenges posed by the 4IR and AI systems in particular.

The South African Law Reform Commission should consider conducting research on the feasibility of enacting digital rights in a single legislative instrument to augment and realise constitutional rights already provided for in the Constitution and other pieces of legislation. The Presidential Commission on AI, together with the Department of Justice and the South African Law Reform Commission should strengthen research into the investigation of the possibility of conferring legal personhood and legal liability on AI systems. Relentless efforts should be made to ensure that South Africa considers clustering various economic sectors, like the financial sector, in order to properly regulate and manage the introduction of AI systems in a concerted manner.

The final recommendation is that the government should consider establishing a public liability company or insurance company to deal with all liability claims emanating from the deployment and use of AI systems.

9 CONCLUSIONS

It has been observed that, apart from contributing to technological advancements, successive industrial revolutions have also impacted both negatively and positively throughout the formalisation and evolution of human rights. This has also resulted in the expansion of science and new technologies, coupled with immense growth in the computational power used in computer hardware and software. Thus has the tone for the 5th Industrial Revolution now been set; it will be dominated by advanced computing and the integration of people with collaborative robotic systems. Many have raised concerns about the existential threat posed by artificial intelligence to human life. The discussion has also highlighted and dispelled the Eurocentric scientific narrative that places the history, development and discovery of technology and artificial intelligence in the hands of white European natives. In challenging this narrative, the argument is advanced that Africa's contribution and account for the origin and development of technology and its impact on human rights can be viewed from the assertion, first, that technology originated in the continent of Africa and, secondly, that the principles and values underlying *Ubuntu* theory have informed the development of human rights theory.

The EU has acknowledged that AI systems are a fast-evolving family of technologies with the potential to bring a wide range of socio-economic benefits across the entire spectrum of the value chain. As a result, the systems are regarded as instrumental to improving prediction and optimising operations and allocation of public goods and resources. While systems play a critical role in supporting socio-economic spin-offs and in improving the welfare of people, they have also given rise to new and nascent human rights issues that need to be addressed by the international community and state actors.

All over the world, states are integrating and deploying AI systems within their apparatus as part of law enforcement, criminal justice, national security

and the provision of other public services. While these AI systems assist in service delivery, concerns are also raised about their dire implications for the protection and enjoyment of basic human rights. As critical economic actors, states are obliged to shape and develop policy and legislative instruments on how AI systems are produced and deployed. This places states as the primary duty bearers in upholding, protecting and respecting human rights in line with international human rights law. This duty entails that nation-states should ensure that both international and domestic laws are applied to the management of both state-owned enterprises, and research-and-development institutions. The same should also be applied to corporate companies as part of mitigating potential harms and damages arising from the production and deployment of AI systems. The rights identified in the discussion are not exhaustive nor is it suggested that they are not currently legislated. Some of these rights are already catered for, although not in a comprehensive manner.

In South Africa, it is critical for the State to consider the enactment of digital rights in a single legislative instrument to augment existing constitutional rights contained in the Bill of Rights. Apart from identifying pertinent digital rights, such legislation may also regulate business conduct and expect robust due diligence from companies in their deployment and use of AI systems ahead of placement in public spaces. A robust due diligence exercise entails overseeing the development and deployment of AI systems by assessing risks and accuracy before they are brought to market. Equally important is to expect developers, programmers, operators, marketers and other users of AI systems within the value chain to be transparent about the details and impact of systems at their disposal. They should instead go further and inform the public and affected individuals about how AI systems arrive at particular decisions autonomously. This should also include notifying individuals about the use of their personal data.