IN SEARCH OF REGIMES OF REGULATION AND ACCOUNTABILITY FOR ARTIFICIAL INTELLIGENCE (AI) IN THE ERA OF THE FOURTH INDUSTRIAL REVOLUTION (4IR) IN SOUTH AFRICA

By

THUPANE JUSTICE KGOALE

[redacted]

Mini-Dissertation Submitted in partial fulfilment of the requirements for the degree of

Master of Laws

in

Development & Management Law

University of Limpopo,

SUPERVISOR: PROF OK ODEKU

ACADEMIC YEAR: 2022

DECLARATION

I hereby declare that this is my original work submitted as my mini – dissertation as part of fulfilling the requirements for the degree, Master of Laws in Development at the University of Limpopo.

This also confirms that the work has not been previously submitted for any degree at this or any other University. Similarly, all the materials and sources used in the completion of this work has been acknowledged accordingly.

Thupane Justice Kgoale

ACKNOWLEDGEMENTS

My sincere appreciation goes to my supervisor Professor Kolawole Odeku for your immensely unbroken support and guidance throughout this beautiful and yet taxing journey. I am greatly beholden to you for having patiently and sensibly directing my research work and continuous dedication in overseeing and propelling this work to its logical conclusion. In the same breath, let me also acknowledge and extend my salutations to none other than Justice Mokgwati Kgaphola, for was always there to give that little push and encouragement. For that, thank you Nape.

I am thankful for the unwavering support from my family and their continuous love and faith in me.

Lastly my gratitude goes to both my workplace colleagues and colleagues in academia, who offered much needed support during the challenging times of completing both my research and coursework.

ABSTRACT

While the deployment and use of Artificial Intelligence Systems (AIS) have continued to grow at an exponential rate in the world, it is assumed that while they have contributed immensely to the economy and society, there is still the problem on how to hold the AIS legally liable and responsible just like a juristic person. The corporate sector in South Africa has intensified the deployment and usage of AIS for their operations. In the process, these systems are susceptible to commits errors and harms thus making it eligible for accountability.

It is against this backdrop of this accountability gap for AIS in the corporate sector that this study explores existing legislative frameworks and other laws to seek to hold AIS accountable. The paper stressed that for there to be a holistic accountability, fragmented legislation for holding AIS accountable should be harmonised for purposes of effective accountability. Especially when it relates to decision-making by both executive management and board of directors. The study has also explored liability and accountability obligations within the entire value chain involved in the creation of artificial intelligence systems as the 4IR occupies a central place in full swing in our lives.

The situation in South Africa is precarious because, presently, the AIS have not been granted clear legal status in any South African statutes. It is pertinent to point out that while there is no legislative framework dealing specifically with AIS and related legal issues in the financial sector such as the banking industry, a raft of legislation is in place to regulate potential risks posed by the use of AIS in the sector in South Africa.

The problem is the fragmented way the regulations and legislation have been approached. To curb the lack of accountability by using AIS in the financial sector, this paper broadly accentuates that to bridge the accountability gap, germane provisions of the Constitution, fragmented legislation, and the jurisprudence from the other jurisdictions where AIS accountability is well developed and have the potential to hold AIS responsible for their omissions or commission was explored and useful lessons drawn accordingly.

Key words: AIS, corporate, accountability, liability, human rights, disclosure

LIST OF ABBREVIATIONS

4.0	: Fourth Industrial Revolution
4IR	: 4th Industrial Revolution
AI	: Artificial Intelligence
AIS	: Artificial Intelligent Systems
AU	: African Union
BEC	: Business Email Compromise
CCTV	: Close Circuit Television
CAHAI	: Council for European Ad Hoc Committee
CIPC	: Companies and Intellectual Property Commission
CODES	: Coalition for Digital Environmental Sustainability
COFI	: Conduct of Financial Institutions Bill [B – 2018]
COVID 19	: Coronavirus
CPA	: Consumer Protection Act 68 2008
CJEU	: Court of Justice of European Union
DABUS	: Device for Autonomous Bootstrapping of Unified Sentience
DAO	: Decentralized Autonomous Organisation
ECJ	: European Court of Justice
ECHR	: European Commission on Human Rights
ECTA	: Electronic Communications and Transactions Act 25 2002

EPO : European Patent Office

EU : European Union

FAIS : Financial Advisory and Intermediaries Service Act

FSB : Financial Services Board

FSCA : Financial Sector Conduct Authority

GDPR : General Data Protection Regulations (EU) 2016/679

GPS : Global Positioning System

GATS : General Agreement on Trade Services

GATT : General Agreement on Tariffs and Trade

ICANN : Internet Cooperation for Assigned Names and Numbering

ICASA : Independent Communication Authority South Africa

ICCPR : International Convention on Civil and Political Rights

IoT : Internet of Things

IMF : International Monetary Fund

LGBTI : Lesbian, Gay, Bisexual, Transgender, and Intersex

MLETR : Modular Law on Electronic Transferable Records

NDP : National Development Plan

OECD : Organisation for Economic Cooperation and Development

PA : Prudential Authority

PC4IR : Presidential Commission on 4th Industrial Revolution

POPIA : Protection of Personal Information Act 4 2013

RIPE : Réseaux Internet Protocol Européens

SEC : Securities and Exchange Commission

SDGs : Sustainable Development Goals

TFEU : Treaty on the Functioning of European Union

TRIPS : Trade – Related Intellectual Property Measures

UDHR : Universal Declaration of Human Rights

UN : United Nations

VITAL : Investment Tool Verification to Advance Life Science

WTO : World Trade Organization

Table of Contents

LIST OF FIGURES

Chapter 1: Introduction and background to the study

1.1 Introduction

As Artificial Intelligence Systems (herein referred to as AI) have grown exponentially and become more sophisticated, there have been arguments that they should be granted some form of legal personality.[1] To illustrate this, Kurki uses a bundle of theory approach in terms of which incidences of legal personality are divided into passive and active personhood, such as infants and adults. In contrasting the extent of the 'bundle of rights' Kurki asserts that infants enjoy certain limited rights while adults are entitled to both full rights and limited ones.[2]

According to Novelli, implicitly or explicitly AI have become indistinguishable from human and as such it should be entitled to a status comparable to natural persons.[3] In this way, AI systems would enjoy legal rights and incur liabilities for damages resulting from possible harms it may cause.

In addition to AI systems and constituting an integral part of the 4th Industrial Revolution (herein referred to as 4IR), other technological innovations critical for the era includes Internet of Things (IoT), robotics, Machine Learning, Blockchain, Big Data, and others with diverse applications. These AI systems are manufactured and produced by corporate companies[4] to incentivize and enhance economic initiatives in

---

[1] Artificial intelligence system is referred to as AI or AIS throughout this study.
[2] Visa AJ Kurki, (2019-08-08). A Theory of Legal Personhood.: Oxford University Press 5 -6.<https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198844037.001.0001/oso-9780198844037. (23 March 2022.)
[3] Claudio Novelli C, Giorgio Bongiovanni & Giovanni Sartor, 'A Conceptual Framework for Legal Personality and its Application to Artificial Intelligence, Jurisprudence, DOI.
[4] The top 10 international companies specializing in AI are Amazon Web Services Inc, Microsoft Corporation, Nvidia Corporation, IBM Corporation, Intel Corporation, Siemens AG, General Electric Company, Oracle Corporation, SAP SE, Robert Bosch Gmbh, Cisco Systems Inc, and Sight Machine Inc. <https://meticulousblog.org/top-10-companies-in-artificial-intelligence-in-manufacturin-market/ (Accessed 24 May 2022). In South Africa

areas of corporate governance, public administration, self-driving vehicles, medical equipment, and digital contracts amongst others.[5] Novelli asserts that the systems operate in an autonomous, intelligent, and smart way without conscious, direct or deliberate human control.[6]

Just like human beings, they are increasingly capable of coping with uncertain and dynamic environments, adapting where there is lack of information, acquiring new knowledge and making appropriate choices.[7] The AI system uses both algorithm and machine learning to function efficiently thus reaching levels comparable to human beings.[8] On the one hand, an algorithm is a set of software rules that a computer follows and implements.

The AI system uses algorithm in computer hardware to function effectively by analysing and evaluating programmed data to execute instructions. On the other, a machine learning relates to the ability of computer software to modify data and operations programming to run predictive models that learns to forecast future behaviours as well as outcomes and trends. What is concerning is that machine learning is susceptible to human errors, depending on the quality of data inputted into the system.

According to Giuffrida et al, AI systems are trained to analyse data which will have dire effects on the validity, accuracy, and usefulness of the information generated by the algorithm.[9] As a set of rule and processes run on internet – linked computer codes to solve a problem or perform a task,

---

the top innovative artificial intelligence companies include Aerobotics, Data Prophet, Explore Data Science Academy, iNNOHEALTH technology solution and Aesthetic and Prosthetic Bionics amongst others. < https://futurology.life/40-most-innovative-south-africa-based-artificial-intelligence-companies/ (24 May 2022).

[5] Novelli 3.

[6] Novelli 4.

[7] Novelli 4

[8] Iria Giuffrida, Fredric Lederer, and Nicolas Vermerys, A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law, 68 Case W. Rsrv. L. Rev. 747 (2018). < https://scholarlycommons.law.case.edu/caselrev/vol68/iss3/14 (14 May 2022).

[9] Giuffrida 747.

algorithms also learn from mannerism and personality of a developer who inputted them into a computer system. Therefore, if such a person is a misogynist, the algorithm would behave likewise.

This must be understood within the context of the entire value chain involved in the AI system. Key to these are merchants and corporate companies that are both hardware and software manufacturers of computers. In turn, these business entities employ the services of software designers, equipment and software installers, facility owners, AI owners, AI users, and trusted third parties, amongst others.

It is pertinent to point out that while juristic persons can be held accountable for actions caused by pre-programmed AI systems such as robots and chatbots,[10] accountability in advanced and autonomous actions of AI systems has become difficult to prove.[11] It is at this point, where issues of liability and accountability kick in. This is significant because decisional processes before pre-programming and compliance with algorithm software rules determine exactly who should be held responsible.

Therefore, clarity surrounding decisional processes that resulted in disregard of algorithm software rules as well as erroneous programming and data input in both the computer software and hardware are very important. In the case of a company, the question will be whether the board of directors sanctioned the action or acted negligently, or conversely whether the AI system acted autonomously and independently without human influence. In this regard, most jurisdictions in the EU and South Africa invoke both strict and vicarious liability rules to hold company directors liable. While product liability laws in both countries regulates this,

[10] A chatbot relates to a computer program that has been designed to simulate conversation with users through artificial intelligence using natural language processing.
[11] Giuffrida 754.

liability for actions emanating from AI systems have proven to be inadequate, as will be shown in this study.

Therefore, the critical question is who should be held responsible for legal acts performed by these systems during the conduct of their routine work. As bearers of legal rights, who between the AI systems and the company that produced it should be held accountable for the legal consequences emanating from their actions? This will depend on whether AI systems are given legal recognition, in which case they would be held liable. In the case of a company, the same applies. If the two have acted or decided jointly, principles of strict or vicarious liability would have to kick in based on circumstances before the courts.[12]

More importantly, how will this affect decision-making processes in corporate bodies if the AI system finally finds its sway and is conferred a legal status in South Africa. If AI systems are granted legal personality, how would law makers and regulators ensure that autonomous intelligent systems and related technologies are designed to obey the same laws as any other persons.[13] The EU has adopted a risk – based approach in its legislative proposals outlining various categories of AI systems and the extend of liability in each category.[14]

Currently, AI systems have not been granted legal status neither in the EU nor South Africa. However, South African patent office has recognized an AI system as an inventor in intellectual property law.[15]

---

[12] Kamalnath, Akshaya and Varottil, Umakanth, A Disclosure-Based Approach to Regulating AI in Corporate Governance (January 7, 2022). NUS Law Working Paper No. 2022/001, <https://ssrn.com/abstract=4002876 or http://dx.doi.org/10.2139/ssrn.4002876 (19 March 2022).

[13] Ameer-Mia, Pienaar and Kekana "South Africa" 248-249; Singh 2020 https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData6_Health_Elec.pdf. (20 March 2022)

[14] The EU Directive, (EU) 2016/680), provides for harmonized rules applicable to the design, development, and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems.

While there is no legislative framework dealing specifically with AI and related legal issues, a raft of legislation is in place to regulate potential risks posed by the usage of AI systems in South Africa.

These include the Constitution and legislation in the areas of banking, consumer protection and health amongst others. The problem is the fragmented way the regulation and legislation have been approached. The Constitution provides in section 8(2) and (3), “that the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, considering the nature of the right and the nature of any duty imposed by the right.”[16] It further requires the courts to develop the common law and its rules to give effect to a right or limit a right in line with the limitation clause contained in section 36 of the Constitution.

These constitutional provisions make it possible to formalize the legal status of AI systems within the armpit of the law. This means that the courts may have to invoke common principles of vicarious and strict liability to recognize the legal personality of the AI systems, if objective conditions obtain. The Courts would have to look at the casual link between the value chain of various role players and harms caused by AI system in order to apportion liability. It should be noted that, absent the necessary legal personality, AI systems may not be directly held legally liable for any harms.

Section 233 of the Constitution empowers the courts to derive guidance from foreign and international law when interpreting any legislation, provided it is consistent with international law. For these reasons, South African courts may have to borrow from approaches developed in the EU

---

[15] Donnelly D "First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in Health Care in South Africa" PER / PELJ 2022(25). < 13.pdf (scielo.org.za). (19 March 2023).
[16] Constitution of the Republic of South Africa 108 1996.

when confronted with questions on the legal capacity of AI systems and legal liability.

In support of these constitutional provisions, various legislative provisions may be invoked to deal with liability issues for AI systems. For instance, section 1 of the Electronic Communications and Transactions Act 25 2002 (ECTA) aims to combat cybercrimes in banking and financial institutions and defines in section 1 automated transactions as electronic transactions. The extent of the validity of electronic contracts is determined within the context of the provisions in this Act. In addition, section 20(c) of the Consumer Protection Act 68 of 2008 (CPA), makes reference to no-fault presumption provisions for product liability arising from defective products and services. The Protection of Personal Information Act 4 2013 (herein referred as POPI) has also been enacted to regulate automated processing of personal information by a responsible party as part of reinforcing the right to privacy and related constitutional rights such as dignity.[17]

This research is intended to the evaluate regulatory environment underpinning AI systems especially in the EU and challenges of accountability facing corporate companies given the uncertainty surrounding the legal status of AI system. Inevitably, this is an era which is bound to disrupt existing legislative framework and legal rules in the 4IR.[18]

According to the European Union report, AI systems are “fast-evolving family of technologies that can bring a wide range of economic and societal benefits across the entire spectrum of political, social and economic value chain.”[19] The systems are regarded as instrumental in

[17] Section 2 of the Act aims to give effect to constitutional right to privacy by safeguarding personal information when processed by companies or organizations subject to certain limitations.
[18] Giuffrida 2.
[19] To this extend, on the 21 April 2021 the European Union Parliament passed the “Artificial Intelligence Act and Proposals for the regulation of the European Parliament

terms of improving prediction, optimising operations and resource allocation as well as personalising service delivery. The use of AI systems plays a critical role in supporting socially and environmentally beneficial outcomes that put corporate companies at key competitive advantage.[20]

To provide an in-depth evaluation of the legal implications of AI systems, the discussion will critically investigate and analyse selected legal sources from the European Union on the one hand, and South Africa on the other. This is significant in that the European Union has established a fairly semblance of legal frameworks for AI, critical for South Africa and African Union to draw lessons from.[21]

While South Africa has some fragmented measure of regulating certain aspects of AI systems, there is currently no specific pieces of legislation and policy frameworks relating to a legal status of these technological beings. Therefore, the research highlights glaring inadequacies within the current South African legal framework insofar as the status of legal personality of AI systems are concerned.[22]

Similarly, existing policy frameworks by the African Union pays less attention to recognition and legal status of AI systems presumably waiting for a signal from the West. The only important continental instrument with relevance to AI is the 2014 AU Convention on Cyber Security and Personal Data Protection, adopted in 2014. According to Gwagwa, only eight AU Member States had signed, ratified, and deposited the convention in 2020.[23] This demonstrates a lacklustre response in terms of

---

and the Council laying down harmonised rules on Artificial Intelligence (herein referred to as Artificial Intelligence Act) and further amending certain Union legislative acts. EUR-Lex – 52021PC0206. < https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELLAR:e0649735-a372-11eb-9585-01aa75ed71a1. (21 March 2022)

[20] Novelli 2.

[21] Giuffrida 12.

[22] Guiffrida 15.

policy and legislative interventions in the continent. Informed by this, a number of African Union Member States had enacted “comprehensive data protection and privacy legislation. Other than this, nothing significant has been put in place. At the national level, few countries have established formal AI strategies while several others have set up task forces entrusted with the responsibility to develop national AI strategies. In addition, many AI-inspired projects and programs are running in various countries coupled with capacity training programs in institutions of higher learning.

1.2 Conceptual clarifications

The concept of corporate governance can be located within the business law parameters. In terms of legal principles underpinning business law, ownership, and control of a company rest with shareholders, company directors and prescribed officers who enjoy certain rights and obligations when it comes to decision making.

To ensure accountability and transparency in the corporate world, four key governance principles were introduced in King III and 1V Reports. The principles include increased involvement of stakeholders, public disclosures by companies, independence of directors and alignment of management of groups of companies. While these principles are not binding, almost all of them are encapsulated in various pieces of legislation such as imperatives of fiduciary duties of company directions in line with section 76 (3) of the Companies Act 71 2008.

According to Damodar, it is not easy to define AI systems because most definitions are unhelpful as they are mechanical and compares it with human behaviour.[24] As a result, Damodar defines it to mean:

---

[23] Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., & De Beer, J. (2020). Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. The African Journal of Information and Communication (AJIC), 26, 1-28. https://doi.org/10.23962/10539/30361. (20 March 2022).

> creating a computer process that acts in a manner that an ordinary person would deem intelligent, and consideration is given to some of the various types of Artificial Intelligence and Artificial Intelligence technologies that might be of concern to people in the digital forensics' community. The legal systems do not have an exact definition of artificial intelligence yet, we have to examine what could be considered as Artificial Intelligence in philosophy and science.[25]

The end of the 19th century witnessed the emergence of the Second Industrial Revolution, which ushered in major breakthroughs in the form of electricity distribution, communication, and new forms of power generation. The era witnessed the development of digital systems, communication, and rapid advances in computing power with their ability to generate, process and share information characterized the Third Industrial Revolution in the 1950s.

The origin of the definition of 4IR is ascribed to Klaus Schwab, who defines it as the fourth major industrial era since the beginning of the first Industrial Revolution of the 18th century.[26] He describes it as an era where individuals move between digital domains due to use of connected technology to enable and manage their lives. He argued that this is an era characterized by a fusion of technologies that is blending the lines between the physical, digital, and biological spheres.[27]

The 4IR represents entirely new ways in which technology becomes embedded within societies and even our human bodies through chips It is

---

[24] Damodar Singh Rajpurohit & Rishika Seal, 'Legal Definition of Artificial Intelligence' (2019) 10 Supremo Amicus 87, OSCOLA 4th ed.
[25] Ibid.
[26] The term was coined by Klaus Schwab in 2016, founder and executive chairman of the World Economic. Schwab K, The Fourth Industrial Revolution. January 2016, World Economic Forum.
[27] Schwab 20 – 22.

exemplified by new forms of machine learning, natural language processing and internet of things amongst others. Through AIs, these novel technologies impact on corporate governance and decision – making in areas of finance, banking, intellectual property and administration of criminal justice to mention a few.

In literal terms, regulation denotes conception and application of legal rules by executive authorities to govern legal relations to ensure uniformity within a given jurisdiction. In the context of AI systems, regulatory responsibilities may be both internal and external, put differently it could be self-regulation or legislative.

Accountability refers to an obligation or willingness to accept responsibility and account for one's actions. As a result, increased access, development, and deployment of AI systems by corporate companies at unprecedented levels impacts of the lives of many people. It is the uncertainties and effectiveness regarding potential risks and harm to users that requires more transparency and openness with AI systems for the sake of accountability.

1.3 Corporate governance accountability

The situation in South Africa is precarious because, presently, AI systems have not been granted clear legal status in any South African's legislative framework. It is pertinent to point out that while there is no legislative framework dealing specifically with AI systems and related legal issues, a raft of legislation is in place to regulate potential risks posed by the use of AIS in South Africa.[28] These include legislation in areas of banking, consumer protection and health amongst others.[29]

---

[28] Section 8 of the Constitution of the Republic of South Africa agitates for the development of common law rules which are binding to both natural and juristic persons within the context of the Bill of Rights. Section 5(1) of the Companies Act 2008 provides for the balancing of the rights and obligations of shareholders and directors in companies in the determination and apportionment of liability issues.

The involvement of various role players in the production of AIS poses critical issues when the moment of accountability and liability obligations arises. In the value chain of these players, the critical question is to point out the person or corporate company responsible for that. In the absence of a relevant legislative framework, it would be a mammoth task to hold anyone accountable.

The problem is the fragmented way the regulations and legislation have been approached. To curb the lack of accountability and foster a culture of impunity using AIS, the discussion broadly accentuates that in order to bridge the accountability gap, germane provisions of the Constitution, legislation and the EU laws have the potential to hold AIS responsible for their omissions or commission.

1.4 Problem statement

The reality of the matter is that AI systems may be conferred legal status and legal personality by certain jurisdictions such as the EU and South Africa. In 2021, the EU released a draft Artificial Intelligence Act to provide for a legal framework regulating AI systems placed in the EU digital single market.[30] Key to this is to ensure that AIS are used safely and complies with fundamental human rights. By failing to provide for the definition of artificial intelligence Bill failed to confer legal personhood to AI systems.

The successful enactment of the EU draft Bill may have an unprecedented impact on corporate decision-making processes thus

---

[29] In addition to the Financial Sector Regulation Act 9 2017, the Conduct f Financial Institutions Bill has been passed by Parliament to consolidate about 13 financial sector laws aimed at protecting customers by promoting fair treatment, trust, transparency, and efficient financial markets while enhancing trust and confidence in the sector.

[30] The Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC (2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}. < https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. (07 February 2023).

posing regulatory, accountability, and liability challenges in corporate law. This could be the case when AIS are used within and as part of the corporate decision–making processes such as on investment decisions and credit applications

The recognition of AI systems as legal persons will have far-reaching ramifications in the legal system if not approached carefully. In the corporate world, it will blur decision-making processes within company governance and executive structures which may as well have potential repercussions for both civil and criminal liability.[31] This would be the case when AIS are used in meetings of board of directors and executive management to arrive at certain corporate decisions. The question would be whether AIS can be regarded as members or an aide of these bodies in their own right, if there is anything like that.

1.5 Hypothesis/Research questions

While the "concept of AI is outperforming humans in every kind of task, it has become impressive to some but also worrying to others. The current consensus regarding the future of AI is split between two schools of thought."[32] In this regard, "the first school is of the opinion that as the potential of AI to surpass human intelligence grows higher, AI should be granted its own legal rights and be subjected to its own personal liabilities." Kurki argues that a strong AI can only be conferred a legal personality status once it begins to act as an entity that can act like a

[31] In "Tomomi Umeda v Tesla Inc, Case No. 5:20-cv-2926, a yet-to-be-decided case in the USA involving a driverless motor vehicle accident that claimed two lives, the court will have to determine if the electric carmaker, Tesla, can be held liable for negligence. The carmaker acceded to the instruction of the teenager to remove a speed limiter in the vehicle, which later crashed and killed the teenager with his friend.

[32] Mattioli, M. (2014) Disclosing Big Data. Minnesota Law Review, 99(2): 535–584, aptly put it that "Much of the rhetoric describing big data's potential for innovation assumes that data can be easily and meaningfully reused and recombined to examine new questions […] Most significantly, big data's producers tend to infuse their products with subjective judgments that, when left undisclosed, limit the data's potential for future reuse. […] These conclusions point toward the need for new policies designed to encourage the disclosure of big data practice." 540 – 541.

human being in a sufficient number of ways.[33] To demonstrate this point, an example is given about a minor who is not entitled to certain rights, only to begin to enjoy these rights when the age of maturity is reached. The same applies to women who are denied certain entitlements, especially in some Muslim countries.

An opponent of AI systems, Chesterman,[34] asserts that arguments in favour of legal personality use instrumental reasons which are based on unstated assumptions about what the future hold. To demonstrate this point, he makes reference the legal status of corporate companies as a juristic person. Chesterman further argues that since there is no category to classify AI systems (at the time when the articles was written), it is better to abandon the debate for future developments when personality would not only be useful but deserved. This second school is of the opinion that legal rights and liabilities should not be extended to cover AI, this simply because the result of programming can be attributed to a human being thus all its actions can be traced back to either a human being or a corporation.

1.6 Points of departure

Amongst others, the research will grabble with the following questions:

Are AI systems advanced and capable enough of being conferred a legal status? What would the nature of that legal status be like as compared to the one endowed on legal and juristic persons?

Does the current legal system in the European Union and South Africa make provisions for the recognition of non-human business entities as

---

[33] Visa AJ Kurki, (2019-08-08). A Theory of Legal Personhood.: "Oxford University Press. <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198844037.001.0001/oso-9780198844037. (20 March 2022).

[34] Chesterman, Simon, Artificial Intelligence and the Limits of Legal Personality (August 28, 2020). 69(4) International & Comparative Law Quarterly 819-844 (2020), NUS Law Working Paper No. 2020/025. 843. <https://ssrn.com/abstract=3682372 (12 March 2022).

legal persons? If none, what are the shortcomings and gaps to clothe robotics with a measure of legal personhood?

The critical question to answer is how the introduction of AI systems affects accountability lines and decision-making processes within corporate companies, as we know them currently in both the EU and South Africa. Critical to this is whether AIS can be afforded a place in the board of directors and the extend of its legal liability if the answer is in the positive. The next question would be who will be held responsible for acts performed by these systems during the conduct of their routine works? Currently, principles of vicarious and product liability are applied to hold accountable for harms emanating from usage and deployment of AIS.

As bearers of legal rights, who between the AI system and the company that produced it can be held accountable for the legal consequences emanating from their actions? The challenge will be on the feasibility of formulating and applying normative systems of laws, as represented by human laws on the one hand and robot laws on the other. Put differently, the central to this, is the question whether AIS can be regulated separately away from the laws that govern human beings.

1.7 Literature review

The continued deployment and application of AI and machine systems in various ways will soon be affecting all aspects of our lives. Firstly, the traditional legal rules to confer legal rights may have to be reviewed to accommodate AI systems into the family of legal persons. Secondly, the inevitable thin line between corporate governance and electronic governance represented by AI systems is bound to impair normal decision-making processes within companies as we know them.[35] Legal rules to 'pierce the corporate' veil may have to be revisited to properly

[35] The Companies Act 72 2008.

determine legal requirements for quorums in board meetings. This may also include redefining principles underpinning delegation of duties as well as business judgement rules in company law.[36] It is against this backdrop that a holistic assessment is required to determine if indeed the legal system will be fully ready to apply the existing law to settle disputes occasioned by the emergence of AI systems in a uniform way.

The vexed question about the legal status of AI systems started in the 1950s, when it established itself as a discipline.[37] In subsequent years, the AI systems gained more sophistication and credibility to an extent that many began to assert that it should be accorded some forms of legal personality as suggested by the EU.[38] In its recent proposals introduced in 2021, the EU classified different categories of AIS in accordance with the extent of risks they pose and how each should be regulated.

According to Novelli, AI systems should be conferred some legal personality status depending on their levels of advancement.[39] He argues that the blurring degree of accountability between corporate companies and AI systems, necessitates calls for recognition of these systems. If

---

[36] Bryson, Joanna J. (2010). Robots should be slave. In Wilks (ed), Close Engagements with Artificial Companions: Key social, psychological, ethical and design issues. 63 – 74. "http://www.cs.bath.ac.uk/~jjb/ftp/Bryson-Slaves-Book09.pdf." (12 March 2022.) Despite his ridiculous views that AI systems should be legally recognized as slaves, Bryson et al. argues that natural persons may try to shift responsibility for civil and criminal actions by blaming defective legal personality of AI systems

[37] Michael Haenlein, A Brief History of Artificial Intelligence: On the Past, Present and Future of Artificial Intelligence, Article in California Management Review, July 2019. Haenlein traces the history of AI to the 1950s when it was recognized as a discipline. In this work, he classifies AI into three groupings i.e., as human inspired, analytical, and humanized according to their cognitive, emotional, and social intelligence.

[38] In February 2017, the European Parliament passed a Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (European Parliament and "urged the Commission to create a specific legal status for robots in the long run, so that the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or interact with third parties independently."

[39] Novelli 25.

there must be such recognition, it will have to be in terms of their categories.

Kurki argues that a strong AI is an entity that can 'in relevant respects act like a human being' and as a result be treated like a legal person if they have the capabilities to substantially influence corporate decision-making and further determine the conclusion of contracts amongst others.[40]

As an opponent of AI systems, Chesterman,[41] asserts that arguments in favour of legal personality use instrumental reasons which are based on unstated assumptions about what the future hold. He further argues that since there is no category to classify AI systems, it is better to abandon the debate for future developments when personality would not only be useful but deserved because the systems capability would have developed and grown in leaps and bounds.

The basis of these arguments is that most "AI systems are indistinguishable from humans and as such they should be entitled to a status comparable to natural persons."[42] It is my considered view that the custodianship of advanced AI systems should be located within a newly created international body like the United Nations, with regional bodies having strong powers to ensure accountability, fairness, and transparency. Accountability for different classes of AI systems may further be spread along these international, regional, and domestic spheres of authorities.

In South Africa, no tangible attempt has been made to embrace and regulate the legal subjectivity of AI systems. However, as indicated below a raft of legislation has been enacted to regulate transactions and activities in the digital space, and not the legal status of the systems.[43] This

[40] Kurki ibid 18.
[41] Chesterman 19.
[42] Novelli 2.

will require South Africa to be innovative by developing and adapting existing AI legal principles to remain relevant and competitive in highly globalized economy.

In the case of Financial Mail v Sage Holdings, it appears to have set out principles for liability arising from actions of non-human business entity in South Africa.[44] The case related to industrial espionage where a device was used to tap conversation at a rival newspaper company. The court had to determine whether a natural person is capable of infringing the privacy and reputational rights of a juristic person, and it found in the positive.

In this case, the weekly newspaper, Financial Mail lodged an appeal in the Local Division to challenge an interdict granted to Sage Holding in the lower court from publishing, disseminating, or disclosing certain business activities and information obtained from an unlawful source, which was later confirmed to be tapping. A journalist from the appellant, Financial Mail, prepared an article that was circulated amongst the publication's editors and later with the respondent, Sage Holdings for a right of reply.

The respondent objected to this article on the basis that it contains false and damaging information which can be detrimental with the potential to result in its downfall. Following a number of discussions and negotiations between officials and representatives of the two parties, the article was canned. However, it emerged later that during the to and fro between the parties, a telephone tapping device was planted in the respondent's offices. The information gleaned from this device was used to supplement the existing article. The Financial Mail, therefore, appealed against the interdict granted by the lower court.

---

[43]Ameer-Mia, Pienaar and Kekana "South Africa" 248-249; Singh 2020 <https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData6_Health_Elec.pdf. (15 March 2022).

[44] Financial Mail v Sage Holdings 1993 (2) SA 451 (A) 25.

When dealing with the matter, the court held that "as a matter of general policy the Courts have, in the sphere of personality rights, tended to equate the respective positions of natural and artificial (or legal) persons, where it is possible and appropriate for this to be done."[45]

The transformative nature of the Constitution appears to be amenable in recognizing the legal status of AI systems. Section 8(3) of the Constitution provides that in interpreting the Bill of Rights to a natural or juristic person the courts must develop rules and common law to give effect to a constitutional right and limitations on the proviso that a limitation is in accordance with the provisions of section 36(1).[46] These provisions may open space for recognition of a non-human business entity.

To demonstrate this, section 1 of the Companies Act 71 of 2008 defines a company to mean a juristic person incorporated in terms of Companies Act, a domesticated company, or a juristic person that have registered before certain period.[47] While this definition sounds a bit restrictive by not providing a room for recognition of AI systems, it can be argued that the courts may resort to section 8(2) and (3) as well as section 233 of the Constitution. The courts have a responsibility to interpret and develop common law when dealing with legislation, provided it is consistent with international law. The two provisions may hold a key in determining the legal status of AIS systems, taking into account the common law, global and foreign trends in conferring or withholding particular legal rights on these systems. This would be the case if the proposed AI Act is indeed enacted into law by the EU and courts in other jurisdiction also rules towards recognition and determination of legal status of AIS.

In recognizing the fluidity, dynamism, and ever-changing nature of common law, the Constitutional court in the Nkala case stressed that its

[45] Ibid at 25.
[46] Constitution of the Republic of South Africa, Act 108 of 1996.
[47] Section 1 of the Companies Act 71 2008.

development must be refocused to be 'abreast with the current socio–economic conditions and expectations. [48] To this end, the court applied section 8 (3) and 39 (2) of the constitution which enjoins the courts to develop the common law to the extent that it is consistent with the constitutional values and further serve to enhance the spirit, purport and objects of the Bill of Rights.[49]

In addition, section 1 of ECTA defines 'automated transaction' as an electronic transaction conducted or performed by means of data messages in which a natural person in the ordinary course of business or employment does not review the conduct or data messages. Similarly, the Consumer Protection Act makes a provision for a no-fault presumption for legal liability of suppliers of goods and services for any harm arising from product defect and failure and the binding nature of automated contracts in Section 20(c). The CPA also places liability on programmers for automated transactions, unless there is a proof that deviation from normal programming protocols took place when the automated contracts were concluded.

Because the AI systems are located in a computer programme, section 1(1) of the Copyright Act 98 of 1979 may become handy in clarifying degree of human influence in directing the actions of AI systems. In defining a computer programme, the provision in the Act characterizes a computer programme as a set of instructions fixed or stored in any manner which, when used directly or indirectly in a computer, directs its operations to bring about a result. While these provisions suggest involvement of a human being in fixing or storing instructions in a computer programme, it is

[48] n Nkala v Harmony Gold Mining Company Limited (Treatment Action Campaign NPC and Sonke Gender Justice NPC Amicus Curiae) 2016 JDR 0881 (GJ). The case relates to a certification by the Constitutional Court of a class action by miners and families of victims who suffered silicosis diseases from various mining houses.
[49] Nkala 199.

at this stage that ability of AI systems to act independently and autonomously from human influence may have to be determined.

The "European Parliament adopted a resolution in 2017 calling on its Commission to consider creating 'a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with rights and obligations especially in cases where robots make autonomous decisions or interact with third parties independently."[50] While the resolution was driven by the need to address accountability gaps arising from AI systems, it was also intended to leverage economic benefits and spinoffs brought about by the AI systems. While there are some significant legal principles developed in some jurisdictions in developing countries, not much has been done to clothe AI systems with some forms of legal rules in the developing countries.[51] However, there is a considerable body of case law reports especially in the US that the courts have dealt with albeit in relation to patents, biometrics and trade secrets involving source codes.

In a matter involving privacy violations and granting of consent for purposes of facial recognition by AI systems, a Circuit Court in the US in the case of *Patel v Facebook*.[52] Facebook launched a feature called Tag Suggestions in 2010, which uses facial-recognition technology to analyze if a user's friends on the platform have uploaded their photos. The technology scans and detects facial images by extracting various geometric data from the eyes, nose, and ears, to create a face signature

---

[50] The European Parliament Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (European Parliament, 16 February 2017) para 59(f).

[51] In the US, the federal government introduced the Algorithmic Accountability Act in 2019 which "at requiring "companies to regularly evaluate their tools for accuracy, fairness, bias, and discrimination."

[52] (740 ILCS 14/) Biometric Information Privacy Act. < https://www.documentcloud.org/documents/6248797-Patel-Facebook-Opinion.html. (15 March 2022).

or map. The technology would then compare these faces, and if there is a match, Facebook may suggest tagging the person in the photo.

As a result of this, users of the platform living in Illinois instituted a class action against Facebook claiming that the facial recognition technology violated the Biometric Information Privacy Act (BIPA), 740 Ill of 2008. In terms of sections 15(a) and 15(b) of BIPA, any person aggrieved by a violation of its provisions may institute an action against any offending party. Based on this, the plaintiffs alleged that by collecting, using, and storing biometric identifiers from their photos without their consent violated their rights. The Circuit Court upheld the allegations by the plaintiffs and ruled that the company can be sued for violation of provisions of Biometric Information Privacy.

At the continental level, the African Union Commission has developed what is known as the Digital Transformation Strategy for Africa which is based on other initiatives and frameworks to create a single digital market in collaboration with other partners by 2030.[53] Amongst others, the Strategy seeks to harmonize policies, laws, and regulations to improve and strengthen intra-investment and capital flows as well as the socio-economic integration of the continent. The Strategy further seeks to promote cross–border open standards and trustworthy AI frameworks, especially in relation to personal data protection and privacy as well as counterbalancing Cyber Security and Personal Data Protection and Privacy issues. In addition, the only key continental instrument with

[53] The Digital Transformation Strategy for Africa (2020-2030) builds on the existing initiatives and frameworks such as the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), the African Continental Free Trade Area (AfCFTA), the African Union Financial Institutions (AUFIs, the Single African Air Transport Market (SAATM); and the Free Movement of Persons (FMP) to support the development of a Digital Single Market (DSM) for Africa, as part of the integration priorities of the African Union. The Smart Africa Initiative has set the creation of a Digital Single Market in Africa as its ultimate strategic vision. < 38507-doc-dts-english.pdf (au.int) (20 December 2022).

relevance to AI is the African Union Convention on Cyber Security and Personal Data Protection adopted in 2014.

The Convention imposes broad obligations on Member States to establish national cybersecurity policies as well as legal, regulatory, and institutional frameworks for cybersecurity governance and cybercrime control.[54] Most importantly, the Convention adopts a technology-neutral language to establish substantive and procedural criminal law provisions which address cybersecurity governance and cybercrime control in AU Member States.

However, as of the end of 2022, only a paltry fourteen Member States had signed, ratified, and deposited the Convention.[55] The Convention requires ratification and signatures by at least 15 member states to become enforceable and binding. A technical team consisting of communication ministers has been set up to further establish a working group on AI, based on existing initiatives and in collaboration with African institutions of high learning. Their brief includes working on the creation of a common African stance on AI, development of an Africa wide capacity building framework, establishment of an AI think tank to assess and recommend projects to collaborate in advancing the goals for Agenda 2063 and 2030 Sustainable Development Goals 2030.

As part of this, “the African Commission Human and Peoples Rights adopted a Resolution calling on state parties to work towards a comprehensive legal and ethical governance framework for AI

[54] The Convention requires, in Article 25 (4), Member States to adopt necessary legislative and regulatory measures against cybercrimes, citizen’s rights, protection of critical infrastructure and establishment of regulatory bodies.

[55] Currently, the Convention has been signed by only 14 member states: Angola, Chad, Guinea – Bissau, Comoros, Congo, Ghana, Mauritania, Rwanda, Mozambique, Zimbabwe, Sierra Leone, Togo, Tunisia as well as Sao Tome & Principe. South Africa has not yet signed the Convention. < https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (02 March 2022).

technologies, robotics and other new and emerging technologies to ensure compliance with the African Charter and other regional treaties."[56]

While acknowledging opportunities and dangers posed by the emergence of AIS in the current digital age, the African Commission on Human and People's Rights echoed similar sentiments and took a resolution in 2021 calling on state parties to act in anticipation.[57] Amongst others, the resolution urges state parties to ensure the development, importation, and use of AIS and other emerging technologies are compatible with the rights and duties as provided for in the African Charter of Human and People's Rights. To this end, the resolution calls on state parties to develop comprehensive legal and ethical frameworks to ensure compliance with the Charter provisions and responds to the needs and values of the people of the continent.

It is not surprising that Africa is found wanting in this important global programme, especially in regard to formal regulation of AIS. It remains to be seen if the continent would be able to catch up in what the South African Minister of Communication refers to as the 'AI race'.[58] Moreover, current efforts are merely aimed at development of policies and guidelines to leverage economic opportunities and prevention of human rights violation. The efforts do not go to the important aspect defining, conceptualizing, and contesting the nature of AI systems so as to avoid possible cyber-colonization. This relates to the failure by the continent to catch up with developed countries such as the EU in regulating AIS.

---

[56] The "African Commission on Human and Peoples' Rights Resolution 473. < https://www.achpr.org/sessions/resolutions?id=504 (26 May 2022.)

[57] Resolution 473 on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa - ACHPR/Res. 473 (EXT.OS/ XXXI) 2021.< African Commission on Human and Peoples' Rights Sessions (achpr.org). (26 May 2022).

[58] Minister Khumbudzo Ntshavheni referred to this during her speech on Africa Ministers of ICT in Namibia on 21 November 2021. <https://www.gov.za/speeches/minister-khumbudzo-ntshavheni-remarks-artificial-intelligence-ai-regulation-while. (26 May 2022).

1.8 Research scope and limitations

The overarching focus of this research is on the South African perspective.[59] To facilitate a critical comparative legal analysis, the legal positions in the EU and South Africa would be evaluated in detail.[60] These jurisdictions are important because they have an established solid base on theoretical exposition of the AI systems, coupled with a widespread adoption of the systems as well as the substantial progress in regulating the AI thus far.[61]

As a highly technical and complex subject matter, the discussion will confine itself to potential implications and challenges of decision making in corporate governance in the light of inevitable recognition of the AI systems as a legal subject within the family of legal persons.[62]

Since this area of law is novel and under-developed, research will be conducted using available international sources of law from other jurisdictions.

1.9 Structure of the research

1.9.1 Chapter 1:

---

[59] However, "according to Giles J & Emma-Iwuoha A 'South Africa Chapter' in A Bensoussan et al. (1st Ed) Comparative Handbook: Robotic Technologies Law (2016) 265, there is no law regulating AI in a more direct way currently."

[60] The White House is also very active in producing policy papers, reports, and other documents (White House, 2012; White House, 2012c, White House, 2014, White House, 2015a, White House, 2016. Similarly, China and Malta have made significant progress in legislating and regulating critical aspects of AI.

[61] In an administrative proceeding, the tribunal In re BlueCrest Capital Management Limited File No. 3-20162, the US Securities and Exchange Commission delivered judgement on 11 February 2021.This is a matter involving conflict of interest and failure to disclose, the US Securities and Exchange Commission ruled that omissions and misstatements to existing and potential investors about the discrepancies of live trading activities was negligent and violation of stock trading rules. In this case, BlueCrest owned the Rate Management Trading, which reported underperformance during live trading at the stock market contrary to the high usage of algorithm at a material time.

[62] This is the case because this is doctrinal legal research which ranges between straightforward descriptions of (new) laws, with some incidental interpretative comments, on the one hand, and innovative theory building (systematization) of the other (Hoecke, 2011: vi).

While the chapter provided how the research is structured, it also introduces the overall research theme as well as its aims and objectives. The chapter outlines the problem question and raises research questions.

In addition, the chapter provides a comprehensive literature review, points of departures and the significance of research. The chapter further outlines the sequence of the chapters in the research. It then ends by outlining recommendations and conclusionary remarks.

1.9.2 Chapter 2: Theoretical frameworks underpinning AI Systems

The discussion in this chapter interrogates theoretical and technical framework informing the operations and machinations of AI. The point of departure is to outline in simplistic terms the technical aspects of AI systems to assess what makes them tick. This is important to enable one to have a thorough understanding of how AI operates technically and technologically.

The discussion undertakes an interdisciplinary approach, combining science and technology, to carve out theoretical and philosophical grounding of artificial intelligence and associated legal implications. This is important to enable one to have a thorough understanding of how AI operates technically and technologically. The discussion defines and identifies existing legal frameworks, guiding values, and principles and whether they properly address all the issues raised by the AI propelled by 4IR.

1.9.3 Chapter 3: International legal instruments regulating Artificial Intelligence Systems

The discussion highlights specific international instruments which have direct and indirect impacts on AI, especially in respect of corporate governance accountability, within the jurisdictional parameters of South

Africa and the European Union. This includes both binding and non–binding instruments. Guidance will also be derived from soft law principles, playing critical role in shaping regulation and governance of AI systems.

Specific human rights regimes vulnerable to AI disruptions are also identified and examined as they may be affected by corporate governance decision making processes are evaluated.

Applicable international legal instruments and regulatory regimes relating to international trade and intellectual property law are also considered. The inextricable link between these areas of law makes it extremely important to address and bring into perspective within the context of corporate accountability.

An evaluation of the legal implications of AI systems is conducted with reference to selected international legal sources in the European Union. To understand the impact and challenges posed by AI, it is also important to examine some of the critical fundamental rights sacrosanct to the basic livelihood of humanity. Central to humanity's livelihood is the impact which AIS has on the conduct of international trade and the global governance of intellectual property.

1.9.4 Chapter 4: Regulation and legal accountability for Artificial Intelligence Systems in the European Union

The Chapter evaluates and assesses regulatory frameworks to hold accountable corporate entities in the European Union. Apart from interrogates existing regional and national legislative and policy frameworks, an indebt assessment of the proposed Artificial Intelligence Act by the European Commission and how this shapes the development of AIS.

Having assessed and reflected on the AI risk – approach envisaged by the legislative proposal, the discussion will focus on liability rules for both product and AI liability in terms of their implications for corporate governance and liability.

1.9.5 Chapter 5: Regulation of Artificial and legal accountability of Intelligence Systems in South Africa

The purpose of this paper is to evaluate existing sectoral legislative enactments and policy framework which seems to lend credence to the feasibility of the recognition of AIS as legal persons. This discussion will also reflect on the impact and challenges companies must grabble with as the emergence of the Fourth Industrial Revolution (4IR) intensifies.

The discussion will further locate executive decision-making processes in business entities and further draw a parallel on how these decisions could be made in the event AI systems are conferred with legal status.

1.9.6 Conclusion and recommendations

A critical comparative study will be conducted and evaluated in detail on the legal position in the European Union and South Africa. While the discussion takes note of developments throughout the worked, active interest is focused on the two identified jurisdictions.[63]

These jurisdictions are important in that they have established a solid base for theoretical exposition of the AI systems coupled with a substantial progress in regulating the AI thus far.

1.10 Research methodology

[63] The White House in the US has been "very active in producing policy papers, reports, and other documents since 2012." Similarly, China and Malta have made significant progress in legislating and regulating critical aspects of AI.

As doctrinal legal research, the study is based on a desktop approach utilizing scholarly sources such as accredited peer-reviewed journals, articles, court case, books including government, international and regional legal instruments.

Most of these sources are located in the University of Limpopo (UL) Electronic Database and online. The research will make attributions to all sources used.

1.11 Significance of the research

The rationale for this study is to make a determination on whether the recognition and conferral of legal personality to AI system a step in the right direction by regulating its legal relationships with natural and juristic persons. This will go a long way in assisting the legal system when confronted with challenges of regulations, accountability, and decision-making processes in corporate governance.

1.12 Conclusion

In this chapter, the scope and background of the study was introduced. The chapter also examined the problem statement and identified research questions for the study, followed by the points of departure. The study further provided a literature review consisting of scholarly works, legislation, case law and government publications. In addition, it also defined key concepts and outlined the significance of the study.

The research will arrive at certain conclusions, informed by either of the assessment of regulatory environment of AIS in the EU. Having assessed the situation in the EU, the study further evaluates the South African legislative policy environment to determine the regulation of AIS. The study would conclude with recommendations which could be taken into

account in the development of legislative and policy framework for AIS in South Africa.

Chapter 2: Theoretical framework underpinning AI systems

2.1 Introduction

Data is new currency and money is data.[64] Data mining and collection stand to be a defining feature of a society dominated by artificial intelligence as we enter the 4IR. According to Forbes, raw unprocessed personal data has economic value and is the backbone of digital retail enterprises as it feeds multiple systems of records to inform a wide range of government and business decisions.[65] In addition to its economic value, it is also imperative that the very same data must be up to date and current in line with prevailing socio – economic imperatives.

The discussion in this chapter interrogates theoretical and technical framework informing the operations and machinations of AI. The point of departure is to outline in simplistic terms the technical aspects of AI systems to assess what makes them tick. This is important to enable one to have a thorough understanding of how AI operates technically and technologically.

In a way, the discussion undertakes an interdisciplinary approach, combining science and technology, to carve out theoretical and philosophical grounding of artificial intelligence and associated legal implications. This is important to enable one to have a thorough understanding of how AI operates technically and technologically. The discussion defines and identifies existing legal frameworks, guiding values, and principles and whether they properly address all the issues raised by the AI propelled by 4IR.

---

[64] Fan, W., Geerts, F. (2012). Data Currency. In: Foundations of Data Quality Management. Synthesis Lectures on Data Management. Springer, Cham. https://doi.org/10.1007/978-3-031-01892-3_6. (20 March 2022).

[65] Forbes Magazine, Why Source Data Is The New Currency For Retailers, Brent Brown, Forbes Technology Council,03 November 2021.< https://www.forbes.com/sites/forbestechcouncil/2021/11/03/why-source-data-is-the-new-currency-for-retailers/?sh=32e0ca855e11.(20 March 2022).

2.2 Definitional impasse confronting AIS

Although the term AI has been in use for nearly 70 years, no universally accepted definition of AI has emerged.[66] It has been accepted that numerous definitions in various texts, policies and statues is indicative that absence of no agreed upon definition shows how elusive AIS are. Most articles have viewed the term as amorphous and capable with many and varied definitions. John McCarthy, who famously coined the term in 1956, opined that since there is no:

> "solid definition of intelligence that doesn't depend on relating it to human intelligence ... we cannot yet characterize in general what kinds of computational procedures we want to call intelligent".[67]

The extensive discussion of the possibility of dressing AI with a legal personality status started with the European Parliament's 2017 Resolution on civil law provisions on robotics.[68] The rationale behind this was based on the need to hold accountable sophisticated and advanced AIS in the event they make advanced decisions or interact with third parties independently. It was then that the concept of electronic personhood, in relation to robotics, began to emerge. It would therefore seem that unsuccessful attempts to define AIS make it more difficult to address its legal personality up to this point.

While the current legislative proposals in the EU seek to answer the primary question through legislation and regulation of AIS, they fell short in

---

[66] Martin Ebers, 'Liability for Artificial Intelligence and EU Consumer Law' (2021) 12 J Intell Prop Info Tech & Elec Com L 204.<https://heinonline.org/HOL/P?h=hein.journals/jipitec12&i=211 (08 October 2022).

[67] Andresen, S.L., 2002. John McCarthy: father of AI. *IEEE Intelligent Systems*, *17*(5), pp.84-85. < https://is.muni.cz/el/law/podzim2020/MV735K/um/ai/REGULATING_ARTIFICIAL_INTELLIGENCE_SYSTEMS.txt?cv=1&session-id=27f7bc71cf4d4b7db73ec6782f044c31

[68] Paweł Nowik, Electronic personhood for artificial intelligence in the workplace, Computer Law & Security Review, Volume 42,2021, < https://www.sciencedirect.com/science/article/abs/pii/S0267364921000571?via%3Dihub. (08 October 2022).

defining the subject itself. In the initial stages, the proposals attempted to assign a definition, but the EU Parliament strategically bowed to industry pressure and exclude it in the final proposals. There is therefore no universal and authoritative definition of the system, even by the European Union which abandoned its initial proposals. The initial proposals defined it as follows:

> a system that is either software-based or embedded in hardware devices, and that displays intelligent behaviour by, inter alia, collecting, processing, analyzing, and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.[69]

By adopting such a wide AI definition, the European Commission aims for providing a general framework to regulate different types of AI without, however, focusing on specific and contextual details. While embracing such a general perspective on AI sets a clear limitation, this wide approach to AI also serves as an advantage by offering the possibility to look at whether this could clash or match with current societal, technical, and methodological boundaries. This would also enable the monitoring of the impact the regulations are making.

The Organisation for Economic Co-operation and Development (OECD) has adopted a similar definition:[70]

> As a machine-based system, AI systems are able to make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are

---

[69] Article 4 (a) of the European Parliament Resolution, Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies (European Parliament), 20 October 2020 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html). Also see European Commission 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN. (29 March 2022).

[70] Recommendation of the OECD Council on Artificial Intelligence. < OECD Legal Instruments. (30 March 2022).

> designed to operate with varying degrees of autonomy, for a given set of human-defined objectives.

This elusiveness can also be seen in most developing countries which are contemplating or in the process of regulating AIS. For instance, in China, another global leader in shaping AI development, there is no clear cut definition of the term. Other countries, too, seem reluctant to crystalize AI further at this stage. In the UK, House of Lords simply refers to AIS as technologies having ability to perform 'tasks that naturally requires human intelligence' and generally have the capacity to 'learn or adapt while acquiring new experience'. This is the general trend adopted by most of these countries, demonstrating reluctance to crystallize AIS at this point in time.

While there is lack of universally agreed definition, it is clear that there are some common denominators amongst global leaders on emerging regulatory approaches on AI. Firstly, they share a consensus that AI is a generic concept constituted by various technologies such as Algorithms, Big Data, Machine Learning, Deep Learning, Natural Language Processing and Robotics amongst others. Secondly, there is also agreement that AIS operate through software (mainly virtually) and hardware devices.

Most importantly, there is general agreement that the 'intelligence' aspect of the concept is context – specific in differentiating Narrow AI and General AI. Narrow AI relates to weak AI which currently dominant and is being used to carry out specific tasks, while General AI refers to AI systems which are intellectually indistinguishable from a human being. Contemporary AI systems include facial recognition systems, credit application systems and autonomous driving systems amongst others. As a results, Narrow AIS have not yet reached the stage of advanced General AI, and this where there is an impasse on coining a definition for AIS that would cloth it with a legal personality status.

These commonalities would go a long way in accelerating processes to design a new legal framework and clarifying legal status of AI systems. The evolution of technological landscape and fragmented approach by international community in developing and defining AI technology holds back the efforts and movement towards regulating the systems.

2.2.1 Impact of definitional defects on emerging autonomous corporate entities

It would seem that developments in the financial and blockchain technology front may offer some glimmer of hope in the conceptualization of the legal personality of AIS. To put it into perspective, blockchains relate to software decentralized technologies which follow rules of formatting and processing protocols that are expressed in a computer code resulting in the invention of cryptocurrencies.[71] Basic blockchain protocols are able to perform simple functions such as exchanging values for Bitcoin or ownership of digital assets through automated smart contracts to perform complex financial transactions amongst others without human involvement.[72]

To this end, various stakeholders including individuals and community groups are then able to invest and trade tokens (Bitcoins) online using blockchain technology. This trading is formalized and takes place through smart contracts known as Decentralized Autonomous Organizations (DAO), created by founders and joined by any stakeholders having an interest.[73] The DAOs have been described as advanced smart contracts

---

[71] Cryptocurrencies are virtual currencies that use decentralized autonomous networks and most popular ones include bitcoin, stellar, polygon, Litecoin and stablecoin amongst others.
[72] Michael Anderson Schillig (2023): Decentralized Autonomous Organizations (DAOs) under English law, Law, and Financial Markets Review, < https://doi.org/10.1080/17521440.2023.2174814. (20 February 2023).
[73] Schillig 12.

that use programmable blockchain protocols to automate transactions and corporate governance through tokens.

The DAOs are created and overseen by developers until they gain membership when their tokens are bought through digital wallets. By acquiring these tokens, purchasers participate fully in its activities which are similar to those of company shareholders and directors. Once they are developed into this form, developers and Bitcoin holders are on equal footing, arriving at decisions collectively according to encoded rules through smart contracts.

It therefore against this backdrop that, in their current form, DAOs raise a number of legal questions. One of the critical questions raised by the formation of DAOs is that there is no separation between ownership and control of the entity when it comes to corporate governance. In addition, they further raise issues of contractual law, data privacy intellectual property, and cybersecurity amongst others.

For DAO members to be held liable, it must be established if they are linked to a limited liability company. Therefore, liability of members will not be capped the DAO is not linked to a limited liability company. In the event of this, debt collect would be source to collect and seize their properties and assets and use their proceeds to satisfy the amount owed by the DAO, including taxes levied on its activities. The only drawback is that there are no incentives for members to take risky business decisions as their personal asserts may be seized by reason of DAO having an unlimited liability.

Another critical aspect to consider is the division and degree of liability obligations amongst and between multiple stakeholders within the value chain. It may not be clear whether the systems caused harms as a result

of manufacturing defect, data collection or malfunctioning arising from negligence or fault.

After its establishment in 1966, the United Nations Commission on International Trade Law (UNCITRAL) was entrusted with the important responsibility to modernize and harmonize international trade targeting key areas of commercial law involving domestic and foreign companies through a non-tariff barrier to trade.[74] As one of the directives adopted by the UNCITRAL in 2017, the Model Law on Electronic Transferable Records (MLETR)[75] legally enables the use of electronic transferable records that are equivalent to sums of money and supports paperless digital trade using crypto assets.[76]

In this way, the MLETR provides for the regulation of blockchain technologies to a particular extent. However, it falls short of including emerging corporate entities, as legal persons, in the form of DAOs. In the current form, the DAOs is faced with difficulties in engaging in credible and legal commercial transactions including tax obligations.

The consequences of this uncertainty regarding its legal status is not conducive for potential investors given the liability risks involved. Similarly, innocent community members and other stakeholders are left with no recourse once funds invested in blockchain business such as DAOs disappears in the hands of unscrupulous developers and founders.

---

[74] South Africa is a member, while certain EU Member States (such as France, Germany, and Israel) are signatories to UNCITRAL. See also Abdellatif, N.P. (2020). An Ethereum bill of lading under the UNCITRAL MLETR. Maastricht Journal of European and Comparative Law, 27(2), 250–274. <https://doi.org/10.1177/1023263X20904316.(15 April 2022).

[75] Article 1 and 10 (1) of UNCITRAL "UNCITRAL Model Law on Electronic Transferable Records" (United Nations, 2017). < UNCITRAL Model Law on Electronic Transferable Records (2017) | United Nations Commission On International Trade Law. (15 April 2022).

[76] Abdellatif 16.

2.2.2 Legal personality challenges in the blockchain and bitcoin enterprises

In May 2022, the disunity in defining AIS came to the fore in the Sarcuni case in the Southern California state in the US where the plaintiff's bone of contention centred on the uncertainties and frustrations stemming from the impasse to define and bringing AIS within the parameters of a legal person.[77] This is a putative class action lawsuit by individuals from various countries regarding the *bZx DAO's* legal status and the potential liability that may arise therefrom.

In this lawsuit, the plaintiffs instituted a claim against the DAO and its co-founders after invested funds were siphoned off in a cyberattack from a decentralized finance protocol. The plaintiffs alleged that developers and founders of the *bZx DAO* were negligent. In addition, they also alleged by failing to create a general partnership, as expected, the defendants *(bZx DAO)* acted as a legal entity in which crypto assets were transferred thus making it a general partnership.[78]

Based on these, the plaintiffs argue that *bZx DAO*, its co–founders and members be jointly and severally held liable for negligence for the theft of approximately USD$55 million in funds from a decentralized finance protocol. It is important to indicate that these co-founders include a number of investments firms.

Central to the plaintiff's arguments is that *bZx* failed to take security measures necessary to protect the funds held in security protocols, despite the fact that such measures were implemented in other partners DAOs. What also ameliorated matters, is the fact that founders of bZx

[77] Sarcuni et al v. bZx DAO et al (S. D. Cal., May 2, 2022 < Sarcuni et al v. bZx DAO et al 3:2022cv00618 | US District Court for the Southern District of California | Justia. (23 January 2023).
[78] Sarcuni Docket & Fillings, Document 1.

promised that such funds would be transferred to a general partnership which is a legal entity before they were siphoned off.[79]

Another important aspect which the court may have to assess is the distinction between ownership and control to determine liability of a decentralized autonomous organization. Realizing the risks associated with skeletal access key to zBx protocol, developers and investors may prefer to be in possession and control of such keys for practical reasons. The courts may also view this as an indication of control in determining liability between and amongst participants.

Determination of liability would also compel the court to assess the nature of the DAO in totality including the threshold of ownership, which may involve original development team, early investors as well as passive users of the underlying protocol and varying degree of individuals linked to the tokens they own or control.

In conclusion, any decision in *Sarcuni* is likely to have wide-reaching implications for legal status of DAO and its participants across the world. If the court answers in the positive, it will imply that artificial intelligence systems in the form of DAOS would be conferred with a status of legal personality with plaintiffs entitled to compensation for their losses. If the verdict goes another way, the status quo will remain leaving plaintiffs with no legal remedy. Similarly, this would also serve as a caution to developers, founders and members of DAOs about their potential liability in future. To mitigate these potential risks, participants in DAOs may have to consider traditional means of protection such as a corporate vehicle as blockers without compromising the flexibility that comes with this kind of a business.

2.3 Theoretical and philosophical postulations of AI

[79] Sarcuni Docket & Fillings, Document 1.

According to McCarthy, the artificial intelligence community and scholarship regard Turing as the pioneer and father of computer science in the 1950s.[80] At the time, Turing had modelled am eponymic test based on a studio game popular by placing a man and woman in separate rooms. They were then made to provide answers to questions in writing to participants who in turn had to guess who answered the questions between the two.

As a result, computers were subsequently used to play similar games and a postulation developed that if machines could fool people they should then be regarded as intelligent.[81] It was this analogy with a natural person which encouraged more research into AI capacity and the extent of its intelligence. Despite abundant evidence that machines could never be human, there was also realization that slaves and women were once excluded from the category of natural persons in their own rights.[82] Therefore, the fact that AIS could be afforded legal status with legal rights and obligations cannot be discounted completely.

Both theoretical and philosophical basis of human intelligence is based on its ability to generate actions, epistemology, consciousness and independent free will. All these elements, at least substantially, mimic what artificial intelligence consist of.[83]

This has raised two schools of thoughts, one embracing development of AI and the other advancing arguments to stem its development.[84] Their

---

[80] McCarthy John. The Philosophy of AI and the AI of Philosophy, 1998. aiphil2.pdf (stanford.edu). (15 June 2022).
[81] Chesterman, S. (2020). Artificial Intelligence and The Limits of Legal Personality. *International and Comparative Law Quarterly, 69*(4), ARTIFICIAL INTELLIGENCE AND THE LIMITS OF LEGAL PERSONALITY | International & Comparative Law Quarterly | Cambridge Core. (20 June 2022).
[82] Chesterman 821.
[83] McCarthy 7.
[84] The study is not focused on varying schools of thoughts regarding AI.

arguments mainly centred around AI existential threat to humanity and the universe, as we know it today.[85]

2.4 AI Compositional framework

A consensus has been established amongst scholars that AI consists of narrow (or weak) and general (or strong) categories.[86] In terms of this categorization, narrow AI is made of algorithms which makes it compete with human thinking and reasoning. Narrow AI is predominantly applied in most automated systems currently in use by corporate companies such as self–driving cars, robots, and stock trading amongst others.[87]

While narrow AI can automate a single activity normally assigned to a human, an advanced general AI can outperform a human being.[88] Because of its capabilities, general AI can therefore be able to solve problems never encountered before by performing new tasks. For these reasons, general AI is regarded as being able to think, and reason and possesses deductive capabilities in more or less the same as human beings.[89]

However, some commentators assert that currently no system has been developed to the level of a status befitting of a General AI.[90] Goertzel asserts that while:

> "narrow AI" refers to the creation of systems that carry out specific "intelligent" behaviours in specific contexts

---

[85] Chesterman 822.
[86] Dickson B, What is Narrow, General, and Super Artificial Intelligence, 12 May 2017 <https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/. (15 June 2022).
[87] Dickson.
[88] Dickson.
[89] Natarajan, P., Rogers, B., Dixon, E., Christensen, J., Borne, K., Wilkinson, L., and Mohan, Sm2021. *Demystifying AI for the Enterprise: A Playbook for Business Value and Digital Transformation*. Productivity Press.
[90] Dempsey James X, Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues, Berkeley Centre for Law & Technology August 10, 2020.

> with some level of human intervention, this is different from naturally General Intelligent Systems such as humans.[91]

Naturally General Intelligent Systems are endowed with capabilities to self-adapt, change their goals or circumstances and learn by generalizing knowledge from one context to another.[92]

According to Dempsey, artificial general intelligence can be understood and located in its definitional form with technologies consisting of the following:[93]The characterization by Dempsey shows that AIS consist of several components systems. In this way, algorithms are key to AI systems as they determine data processing procedures while performing their tasks. It is at this point that concerns about privacy and transparency in its decision–making processes arise.

Firstly, algorithms define the rules and procedures for data processing to enable AIS to carry out particular tasks. However, how these algorithms are processed is shrouded in secrecy as there is no transparency, a matter to discussed elsewhere in the chapter. Secondly, in its training Machine Learning utilizes data to identify correlations and assessments of conduct or events which are similar. For instance, the conduct may relate to an individual's propensity to act in a certain way such as the possibility of parolees repeating their offenses after they are released. In the case of events, this could be how a motor vehicle reacts to avoid potential accidental situations.

The third component, Deep Learning, is critical for algorithms to define what features in a dataset should be analysed to arrive at an accurate prediction. Deep Learning combines machine learning and artificial

---

[91] Goertzel, Ben. "Artificial General Intelligence: Concept, State of the Art, and Future Prospects" Journal of Artificial General Intelligence, vol.5, no.1, 2014 1-48. <https://doi.org/10.2478/jagi-2014-0001. (17 April 2022).
[92] Goertzel 4.
[93] Dempsey 6.

intelligence by mimicking how knowledge is obtained by humans, as part of statistical and predictive modelling.

Fourthly, the Neural Networks are responsible for connecting networks and programs used by Deep Learning to roughly approximate neurons in the brain, what is known as ‘black box’. It does this by analysing inputs which enables AIS to make predictions. In the event the Neural Networks gets its predictions wrong, the deep learning algorithm would come on board and adjust the connections among the neurons until there is improvement of prediction accuracy.

Lastly, the Natural Language Processing component enables the AIS to process and interpret both written and spoken human languages in order to function in an expected manner. This is mostly experienced through bots or chat boxes which are used to conclude online contracts and credit applications amongst others. The legal significance of this is about the validity of such contracts, whether the contracts are entered into between an individual and a business enterprise or, conversely between an individual and an AIS in its own right.

Arising from this characterization and definitions, it is clear that both machine learning and deep learning techniques require huge computational power which derives from the availability of big data.[94] It is at this point that major legal and policy issues become critical. Questions of data transparency and duty to disclose determine what is known as algorithmic discrimination.[95] The connection between data collection and the creation of algorithms determines how machine learning techniques operate.

[94] Dempsey 6.
[95] Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI, Opening the Black Box or Pandora's Box, Communications of the ACM.

There have been concerns that data that has been collected is sentient and may reincarnate the personal traits of a collector. If, for example, data was collected by a trigger–happy individual the likelihood is that a robocop will adopt such traits. In criminal law terms, it will call for interrogation of issues of *men's rea and actus reus*, which are requirements for criminal liability. If the AIS lacks mental capacity to commit an offence, then the company, software programmer or a user linked or owning such a system may have to be held accountable. This would then bring into the fore the importance of fault – based liability in the law of delict.

However, it has been argued that the large amount of data located within algorithms also make the AI able to solve problems that humans cannot solve, including human error and biases. An example could be when an AI-based automobile avoids a vehicle driven by a drunk driver. This assertion is not convincing especially given decisions that have been made in autonomous vehicle, credit applications and criminal sentencing procedures using AI-based assessment programs.[96]

It has been proven that some of the manufacturers AI propelled vehicles are not transparent and truthful as they claim. In the US, a Tesla autonomous motor vehicle crashed in 2016 killing a sole occupant who was also a presumed driver.[97] An investigative crash report by authorities revealed that the vehicle was not a self–driving car as claimed in various advertisements by the company.[98] The data extracted from the vehicle also suggested that its owner was behaving as if were an driver. Other crashes which were investigated subsequently further revealed that these

[96] The Annexures 1 – 9 on The Proposal for the Regulation of the European Parliament and The Council Laying Down Harmonized Rules on Artificial Intelligence (Draft Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, 21 April 2021. < resource.html (europa.eu) (24 December 2022).

[97] Tesla driver dies in first fatal autonomous car crash in US, Alice Klein, 1 July 2016. Tesla driver dies in first fatal autonomous car crash in US | New Scientist (15 December 2022).

[98] Stilgoe, J. How can we know a self-driving car is safe? *Ethics Inf Technol* **23**, 635–647 (2021). <https://doi.org/10.1007/s10676-021-09602-1. (24 December 2022).

collisions were not just as a result of carelessness by developers, but a lack of consensus on risk assessments and regulatory standards to hold companies accountable and liable for their deeds arising from AIS.

When combined artificial intelligence shares many things with the Internet of Things and robotics although they do not mean the same thing. Both the Internet of Things and robotics can be described as products of AI in their different ways. To work to the optimal, they can perform tasks independently from human control through network connectivity. Having engraved within the AI systems, they can improve their performance by learning the environment in which it is operating. The technological ecosystem of AI consists of various components, parts, software, and systems which makes it have the capacity to replenish, update and upgrade after it is placed in the market.[99] It is within this context, that the decision–making processes of AI are examined below:

2.5 Decisional processes propelled by AI

While an observation has been made that AIS involve a human element, it is also possible that they may replicate or human errors and biases inherent in a human. An example of this may be when a self-driving vehicle is faced with ethical choices that humans can easily process when a pedestrian is about to be hit by a car. While a human driver may choose to jump a red traffic light, an autonomous vehicle may instead hit a pedestrian. Similarly, a software powered by AIS used to allocate police resources may choose to allocate such resources in leafy suburbs instead of squatter camps which are crime hot spots due to inherent biases in policing patterns. Therefore, this shows that AIS trained on data that reflects biases based on past decisions could incorporate those biases into future decision-making processes. While this may be apportioned to a

[99] EU Commission, 2020. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things, and robotics. COM (2020), 64.

defective product, thus bringing to the fore product liability, it may be difficult to prove liability by virtue of ubiquity and opaque nature of processes underpinning algorithmic composition and orientation as indicated above.

These technological and technical complexities pose challenges especially when it comes to apportionment of legal liability and accountability in order to continue to hold corporate companies accountable. What is also challenging is that human programmers may not be able to fathom how a neural network arrived at its predictions.

The digital economy of the 4IR remains to be dominated by a host of key merchants and corporates within staggered and linked value chains. According to Benhamou emerging digital technologies, including AI, are becoming increasingly complex due to the:

> interdependency between their different components such as i) the tangible parts/devices (sensors, actuators, hardware), ii) the different software components and applications, to iii) the data itself, iv) the data services (i.e. collection, processing, curating, analysing), and v) the connectivity features21. The number of stakeholders involved in the creation and operation of AI systems is concurrently rising: hardware manufacturers, software designers, sellers, equipment and software installers, facility owners, AI owners, AI users and trusted third parties, amongst others, may all have a role to play in ensuring that AI does not cause harm, and allocating liability in this context is not an easy task.[100]

All of these have a clear responsibility to ensure that AI systems enjoy smooth sailing in minimizing and averting causation of harm and consequently legal liability. This means that companies and service providers for these systems can be held liable for failing to update,

[100] Benhamou, Yaniv & Ferland, Justine. (2020). Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages. < (7) (PDF) ARTIFICIAL INTELLIGENCE & DAMAGES: ASSESSING LIABILITY AND CALCULATING THE DAMAGES (researchgate.net). (2022).

replenish and maintain their systems. Given the existing liability regimes in the EU and South Africa, it would be an uphill task to properly identify and apportion liability to any of these players in the context of AI.

It is for this reason that the EU Proposals emphasize the requirement of explainability, in addition to transparency and duty to disclose, as will be shown in Chapter 4.[101] However, explainability considerations may, for instance, be scuppered by intellectual property claims when developers are required to elaborate underlying algorithmic databases. This would be case where companies are reluctant to disclose exact owner of an intellectual property right where AIS was involved.

Another challenge is that there is a growing body of literature questioning the reliability of AI systems for certain applications, including the OIS systems. Similarly, there is currently another body of research which is uncovering how AIS are vulnerable to adversarial attacks.[102] However, Akhtar et al dismiss these assertions and argues that the manner of collection, management and processing of unquantified data may result in false alarms leading into wrong decisions by AIS detecting cyber-attacks.[103]

While the subject of Artificial Intelligence Technologies is complex and technical, legal practitioners, regulators, and policymakers must be familiarised with both technical and technological aspects having potential for legal consequences. This will go a long way in locating and determining fault and liability in AIS matters requiring adjudication by relevant bodies.

2.6 Automation and algorithmic processing

[101] EU Commission Report 10.
[102] Akhtar, Muhammad Shoaib & Feng, Tao. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. EAI Endorsed Transactions on Creative Technologies. < https://eudl.eu/doi/10.4108/eai.23-11-2021.172218. (16 April 2022)
[103] Akhtar 6.

Automation is key and integral part of AIS, which is powered by algorithmic processing of data. The decision-making processes of an AI system lie in how the algorithm processes data. For an automated computing system to work to the maximum, there must be a large-scale data processing capacity able to operate with speed. Because of the volume and scale of AI capability, the data– – driven decision-making processes may end up with lowering error rates as compared to where a human is involved. This could be the case where AI systems are used to assess the creditworthiness of an applicant or even facial recognition devices are used to search and identify suspects.

These automated decision-making algorithms in all AI systems range ranges from simple ones to complex ones. Simple one includes those that are used online by service providers for marketing, while complex one refers to models that are used in filtering systems and offer personalized content. Respectively, simple ones also include chat boxes while complex ones relate to cookies and filtering available when locking to a particular website for instance.

The flighting of cookie banners on electronic gadgets has been met with controversy, especially with regard to the solicitation of informed consent for individual data collection. Two issues raised by this related to the purpose for which data is collected the and legality of sharing such data with third parties. Cookie banners are utilized by website owners to to evaluate user surfing behaviour and interest for advertising purposes. In most websites, users are required to tick pre-selected checkboxes giving consent to use their data before viewing the site. The data collected in this way is then used for advertising and, in some instances, shared with third parties for their own economic purposes.

In 2019, the European Court of Justice dealt with the pre – selected cookie banners in the *Planet49* case.[104] In this case, the dispute related to online

promotional lottery by Planet49 requiring users to provide their personal details on a cookie banner. The first explanatory banner, with a checkbox, required users to click to participate for free of charge. It also required users to give permission to be contacted by third parties for advertising purposes. The second checkbox had a compulsory pre – selected tick box for users to grant consent for their personal data to be used for analytics of surfing behaviour to be used for advertising.

In its judgement, the ECJ ruled that a pre–selected checkbox for cookie banners does not offer consent in terms of the GDPR and ePrivacy Directive. The court reasoned that Article 4 (11) of the GDPR is unambiguous in outlining active consent as it requires individuals to give clear statements and affirmations signifying their consent. In addition, the court held that the GDPR silence or ignorance of such checkboxes does not presume consent and as such only active conduct of a data subject meet the requirement consent to cookies.

Furthermore, the court held that the information which the website service provider is supposed to be given to a user should include “the duration of the operation of cookies and whether or not third parties may have access to those cookies”. Following this judgement, the German Federal Court of Justice went further and held that a “request for consent by a preselected tick box constitutes an unreasonable disadvantage to the user".[105]

Data analysis of algorithms take place when there is a correlation pattern within the databases and are subject to the availability of a massive scale of data. It is important to note that concerns may be raised because of

---

[104] Planet49, CaseC-673/17 1 October 2019, ECLI:EU:C:2019:801. For the headnotes to this decision see this issue of IIC (n11) < https://doi.org/10.1007/s40319-020-00926-x. (24 December 2022).

[105] Federal Court of Justice on consent to telephone advertising and cookie storage, 28 May 2020.< https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html?nn=10690868. (24 December 2022).

errors following the use of pattern recognition due to a misunderstanding of their correlation or causal relationship. As a result, the use of pattern recognition without understanding their correlation or causal relationships may lead to errors and raise concerns about data quality. In this way, the question is whether AIS is used as a decision maker or as a support to corporate decision – making. Similar, if it is used as a support, it may also be argued that it performs delegated functions, which may attract legal consequences.

This is important because the quality of data collected and used in the algorithms determines the existence and extent of harm and biases within the entire system. Datamining relates to the production of data using source codes, which consist of a host of zero representing a particular character, symbol, or language amongst others. The interplay between interplay between applied analytics and the data sets influences automated decision–making processes. To make it simple, Wrobel has outlined how algorithmic decision–making works thus:

> An AI system is first and foremost rational. It achieves rationality by perceiving the environment in which the system is immersed through some sensors, thus collecting and interpreting data, reasoning on what is perceived or processing the information derived from this data, deciding what the best action is, and then acting accordingly, through some actuators, thus possibly modifying the environment.[106]

It is this possibility to modify the environment, which is worrisome, especially in the light of the fact that the AI space is currently dominated by mainly powerful countries in the developing world. And most of these countries are developing the AI systems based on their values and narrow

[106] Wróbel, I. M. (2022). Artificial intelligence systems and the right to good administration. Review of European and Comparative Law, 49(2), 203–223. < https://doi.org/10.31743/recl.13616. (12 January 2023).

national interests and not necessarily for the benefit of entire humanity. This is discernible from the speech by EU President (Ursula van der Leyen) in 2019, which advocated for digital sovereignty, at least with respect to global geopolitical issues.[107]

2.7 Challenges posed by AIS liability frameworks

Having discussed technological and computational aspects of AI systems, it is imperative that we dissect legal challenges and implications that makes its regulation difficult. Some of the main legal issues posing challenges for claims occasioned by operation of AIS relates to causation, foreseeability and autonomy as reflected below.

2.7.1 Causation and foreseeability constraints

One of the key characteristics of AIS is its ability to act autonomously in carrying out complex tasks, with no active human control and supervision. This autonomous capability is expected to continuously increase going to the future accompanied by economic challenges and disruptions in the labour market and other spheres of life as was the case during earlier Industrial Revolutions. As a result, this will force comparably disruptive changes in law as the legal system would find it difficult to cope with the increased ubiquity of AIS.

One important characteristics of an AI which poses a challenge to the legal system relates to the concept of foreseeability. The computational power available in the black – box of certain special AI software together with AI's freedom from the cognitive human biases makes them more capable than ever. The fact that they are able to generate solutions that a human would not expect or foresee, points to the fundamental difference between human decision-making processes and those of modern AI

[107] Mark Sctott, What's driving Europe's new aggressive stance on tech, 28/10/2019, Politico. < What's driving Europe's new aggressive stance on tech - POLITICO. (12 January 2023).

systems. This is due to the cognitive limitations of the human brain, which struggles to analyse massive information at hand when faced with time constraints.

It is precisely this ability to generate unique solutions that make the use of AI unpredictable and unforeseeable, as they are capable of producing actions beyond what systems designers and operators intended for.

Therefore, unenforceability and causation which would make it unfair to hold liable systems designers and operators for any harm caused by AI systems. Similarly, a possibility exists that victims of such harm may not be able to institute proceedings for compensation for their losses. Therefore, issues pertaining to foreseeability and causation present a vexing challenges that the legal system will have to contend with to find redress for victims of AI-caused harms and losses.

2.7.2 Autonomy and control problems

Apart from autonomy which encompasses foreseeability problems, AIS also poses risks of control. Human control of machines that are programmed with considerable autonomy is bound to be difficult. In this regard, loss of control may be due to malfunctioning, flawed programming, corrupted file, or damage to input equipment amongst others.

Because AI systems are designed to learn and adapt, it may also prove difficult to regain control once lost, thus making it a potential source of public risk. This means that a human or humans who are legally responsible for its operation and supervision would have lost control of the systems, which may inadvertently cause harms and damages. As a result of this control and autonomous element over AIS, an increasing number of technopreneurs, futurists and academics have expressed reservations about the catastrophic and existential risks to humanity.[108]

The concerns in question are based on the fact that sophisticated AIS may improve its hardware and software programming to the extent of surpassing human consciousness and cognitive abilities.[109] However, this is dispelled by Russell et.al, who reason that to "minimize human suffering", ex-ante action would be necessary to ensure that the systems remain either susceptible to human control, aligned with the public interest, or both.[110] It is therefore clear that one of the effective tools to maintain and sustain human control is through a legislative instrument.

2.7.3 Opacity and transparency concerns

From a regulatory standpoint, some of the most problematic features of AI relates to the manner in which research and development is conducted. Central to this, is the whole question of transparency concerns which are occasioned by discreetness, diffuseness, and opaqueness surrounding the development of AI systems.

For purposes of our study, discreetness refers to the limited visible infrastructure regarding the conduct of AI development work. This is also connected to claims of intellectual property rights which are often invoked around the manufacturing of various components of AIS. This is despite the fact that separate components of an AI system could be designed in

---

[108] S Akash, AI, the Biggest Existential Threat to Humankind says Elon Musk, Analytics Insight,14 July 2021. <AI, the Biggest Existential Threat to Humankind says Elon Musk (analyticsinsight.net). (Accessed 18 January 2023).

[109] Dr. Roman Yampolskiy, a computer scientist from Louisville University, believes 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. Not being able to control super-intelligent systems could be disastrous. Similarly, Yingxu Wang, professor of Software and Brain Sciences from Calgary University disagrees, saying that "professionally designed AI systems and products are well constrained by a fundamental layer of operating systems for safeguard users' interest and wellbeing, which may not be accessed or modified by the intelligent machines themselves. Eva Hamrud, AI Is Not Actually an Existential Threat to Humanity, Scientists Say, 11 April 2021.< AI Is Not Actually an Existential Threat to Humanity, Scientists Say: Science Alert. (18 January 2023).

[110] Stuart J. Russel & Peter Norvig, Artificial Intelligence: A Modern Approach, 1034, (3d ed. 2010).

different places at different times without any conscious coordination. Secondly, diffuseness relates to the possibility of diversified spread of individuals who may be located far from each other working on a single component of an AI system.

According to O'Reilly, the opacity and unpredictability have led many to express reservations about algorithmic decision-making processes and techniques used in the automation of data.[111] This is especially the case when the filtering bubble for marketing shows more preferences for consumers and less on the quality of products at offer. In a way, this could result in deceiving consumers thus resulting in action for delictual remedies. Similarly, this has also resulted in biases and discrimination based on race and religion in more recent cases.

Finally, the fact that the inner workings of AI system may be kept secret and not susceptible to reverse engineering results in its opaqueness. While these features may be shared through research and development, the technologies involved present particularly unique challenges.

While it is not necessary for a person to have fancy resources and facilities of a large corporation to compose computer codes, anyone with a modern personal computer or even a smart phone with internet can contribute to projects involving AIS. Therefore, individuals can participate in AI development from open – source libraries at any place or location anonymously, without being part of any organization.

While the inner workings and interactions between the components of an AI system may be far opaquer and easier to acquire, their coding is often

---

[111] O'Reilly Tim, "The great question of the 21st century: Whose black box do you trust?", 13 September 2016, available at: < https://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly/?trk=eml-b2_content_ecosystem_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1.(12 January 2023).

proprietary thus bringing to the fore intellectual property issues. This makes critical features underlying the operations of AIS non – obvious and consequently readily susceptible to reverse engineering.

The sheer number of individuals and firms that may participate in the design, modification, and incorporation of an AI system's components makes it difficult to identify the most responsible party or parties in the event of harms or losses occurring. Some components may have been designed years before the AI project was even conceived, and the components' designers may have never envisioned that their designs would be incorporated into any AI system that caused harms or losses.

In such circumstances, it may seem unfair to assign blame to the designer of a component whose work was far removed in terms of both time and space. The courts may be hesitant to conclude that the designer of such a component could have foreseen the harms or losses in question. Similarly, the opaque nature of AI systems may contribute to the reluctance by the courts to find against end – users that causes harm to third parties. Apart from considerations of foreseeability, the multitude of potential defendants will further complicate the assignment and apportionment of liability. These difficulties associated with regulating AI *ex ante* will also complicate efforts to ensure that victims receive compensation *ex post facto* when AI systems causes harm.

2.8 Determining corporate liability regime for AIS

Inarguably, AIS has introduced key socio–economic benefits in society especially in areas of administration of justice, finance, health, and climate change as well as increased productivity and operational efficiency at workplaces amongst others. While it has reduced risks of injuries and damages compared to humans, it has also resulted in undesirable and

sometimes serious consequences such as violation of fundamental rights and fatal accidents during its deployment.

Initially, the task of establishing liability for damages caused by AI used to be rather straightforward. This was because predetermined decisions were limited by human programmers. This has now changed as several stakeholders are involved. Amongst others, the stakeholders in question include sensors and hardware, software and applications, and data programmers and this creates legal difficulties to apportion liability.

The continued development and improvement of AI capability to make autonomous decisions without human supervision further poses challenges in assessing liability for AIS. This is also aggravated by non – the conferral of legal personality to the AI systems by various jurisdictions such as the EU and South Africa. As a result, existing legislative and policy frameworks adopted prior to AI technology are used by the courts and other adjudicatory bodies in an attempt to resolve liability issues.

One of the challenges for AI liability is the lack of sufficient degree of autonomy and intelligence similar to a human, thus making the application of principles of vicarious liability inapplicable. Vicarious liability imposes strict liability on a person or principal for the wrongdoing or negligence of a legal agent, thus making it difficult to determine the reasonable man's test. As things stand, AIS cannot be regarded as an agent as there is no jurisdiction that has conferred with a legal personality status.

This has therefore left tort liability and product liability as the most relevant liability regimes applicable to AIS. The tort liability is fault based and kicks in the moment a civil wrong is committed by one person against another where there is a failure to take reasonable care to avoid injury or loss.

In some civil and common law jurisdictions, like South Africa and many in the EU, the burden of proof lies on the plaintiff to prove a breach of duty.

After having proven breach and establishing fault, the plaintiff must further prove damage suffered or loss incurred. The plaintiff must also establish a causal link between the fault and damages caused or loss suffered to justify compensation.

In the case of AIS, tort law can be applied in instances where presiding officers relies on AI decision support software to convict the accused only to find out that such software was flawed. To be successful, the accused must prove that software issues should have been noticed and were ignored by a reasonably competent officer of the court thus making the presiding officer liable for resultant foreseeable injuries or losses, despite recommendations by the AIS.

Another liability regime relates to product liability, which is concerned with manufactures of finished products, including its raw parts or components. In addition to manufactures, liability may also be apportioned to importers, designers, distributors, suppliers, and retailers of such finished products in broad terms. Apart from holding one party liable, parties can also be held jointly and severally liable for damages and losses caused taking into account the closeness and connection to the harms in question.

As a result of manufacturing defects as well as design defects coupled with failure to warn users against inherent non – obvious dangers of the product concerned, product liability may be invoked to claim damages and losses suffered by complainants. In the European Union, product liability assumes a form of strict liability character.[112] Product liability can be invoked when the usage of a defective product causes damage or loss to consumers or their properties.

The burden of proof lies with the injured person to prove the damage, defect, and causal link between the damage and defect. Once the burden

[112] Articles 1 and 4 of the EU Product Liability Directive.

of proof is fulfilled the manufacturer or producers is then put under a legal duty to compensate the complainant, regardless of existence of negligence or fault on their part.[113]

To assess implications for legal liability and accountability, the hidden impact of applied analytics and the data set effect must be taken into account, for example. The varying degrees of discretionary powers of designers of data and algorithm is also important when assessing biases and the human rights impact of AI.

Based on information and date from various websites, which propagated false information, Google algorithms erroneously referred to Barrack Obama as a Muslim and not as a Christian he is.[114] Another example is a Microsoft chatbot known as Tay, which was interacting with human beings on Twitter and suddenly exhibited its racists behaviour.[115] In these two instances, the algorithm was clearly oriented and trained on polluted data which was possibly based on offensive and racist data gathered from various websites and processed by programmers with a particular mindset.

There is a consensus amongst scientific community that automated decision-making is embedded in algorithmic systems, though with a semblance of the human element. At this point, these systems are manufactured, produced, and owned by mostly AI companies who in turn market and sell them to their clients. As this represent a cyclical commercial transaction between and amongst corporate bodies, it may

---

[113] Ibid.
[114] Jason lemon, Google thinks Obama is Muslim, 19 January 2017. < Step Feed (12 January 2023.
[115] Mark Asquith, Tay Tweets: How far have we come since Tay the twitter bot, 11 October 2018.< Tay Tweets: How Far We've Come Since Tay the Twitter bot (hubtype.com). (12 January2023).

prove difficult to pinpoint where liability lies in the event AIS results in legal consequences.

An AI system may be a single software used for profiling suspects or for producing a medical recommendation to a patient. It can also be used as a credit score system to determine whether a person qualifies for a loan and further to select a suitable curriculum vitae for a position amongst others. Given the complex nature of autonomous systems, existing liability laws appears to be inadequate to provide for recourse for anyone claiming under product liability.

As a result, decision–making processes within corporate governance is critical in determining liability for legal claims where AI systems have been deployed in various transactions. These systems can be used in two ways. Firstly, they can serve as support to executive management or the board of directors by way of recommending certain actions or decisions. Secondly, they can operate autonomously, especially in respect of autonomous vehicles.

How a company's board of directors arrives at a particular decision involving manufacturing and data collection methods is decisive in pointing out a person upon whom liability rest. In cases of deployment of ordinary AI, the decision is simple as the company would be held liable. It is only the deployment of advanced AI systems that poses difficulties, and this is where legislative lacunae become more visible. While the National Credit Act attempt to address this in South Africa in terms of product liability for instance, more still need to be done to adequately provide for liability for AIS. This matter is discussed fully in chapter 4 and 5 of this study.

Legislative and liability regimes are supposed to be well-positioned to respond to this reality. While regulating the production and use of AI systems, proper laws are enacted to compensate victims of harms caused

by these products and, in turn, encourage producers to avoid potential harms. Liability regimes can be generally applied to the corporate sector internationally across all jurisdictions. However, the fact that the exact form and extent of liability regimes may vary substantially across jurisdictions and circumstances, makes legislating AI more important and urgent.

It is this opacity and unpredictability which many believe there is great potential for human rights violations. The vulnerable rights include the right to equality, privacy rights, and fair trial rights amongst others. While the UN acknowledges the technological revolution brought about by the AIS in the light of Sustainable Development Goals, it also expressed its reservations, especially on ethical and human rights implications on a vast number of fundamental rights.[116] To this end, it has mandated UNESCO to coordinate global dialogue on these matters.

2.9 Conclusion

The discussion traced the origin as well as subjective and objective intelligence of AI, informed by its theoretical and philosophical underpinnings. The ability of AI to process data, information, letters, characters and symbols expressed in coding in accordance with set of instructions held in its memory was also evaluated. From the discussion, it is clear that AI is a multi – disciplinary subject rooted in the study of algorithm and big data structures using its technique from queuing theory, statistics and probability through hypothesis, testing and experimentation for its effectiveness.

The distinction between narrow and general AI demonstrates the extend of capability and as a yardstick possibly to be used to measured

[116] Audrey Azoulay, Towards an Ethics of Artificial Intelligence, New Technologies: Where To, December 2018, Vol 3 & 4, < Towards an Ethics of Artificial Intelligence | United Nations. (14 January 2023).

apportionment of liability and accountability when regulatory frameworks are put in place. While the discussion further places data mining and collection as key determinants of sociological basis of algorithm make – up, it also raises question on issues of data justice and transparency.

The discussion will now focus on possible international instruments that can be used to hold accountable regulatory regimes for AI.

CHAPTER 3: International legal instruments regulating AI

3.1 Introduction

All over the world, states are integrating and deploying AI systems within its apparatus as part of law enforcement, criminal justice, national security and provision of other public services. While these AI systems assist in service delivery, they also raise concerns on human rights issues.

Algorithms are key as they are used in forecasting and analysing large quantities of data to assess the risks and predict future trends. The data in question may relate to crime hot spots, social media posts, communication data and the provision of social services amongst others. To complement states, corporate companies are at the forefront of manufacturing and producing a chunk of AI systems which in turn is traded to public authorities. As a critical economic actors, states are obligated to shape and develop policy and legislative instrument on how AI systems are produced and deployed.

This places states as primary duty bearers to uphold and respect human rights in line with international human rights law. This duty entails that states should ensure these laws, together with domestic laws, are applied across the management of State-owned enterprises, research and development funding as well as private corporate companies and vendors to mitigate harms and damages arising from production, marketing deployment of AI systems.

Part of this includes requiring responsible business conduct and exercise of robust due diligence. 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 the market. Equally important is that developers, programmers, operators, marketers, and other users of AI

systems within the chain are expected to be transparent about the details and impact of systems at their disposal.[117] Instead of ending here, they should go further and inform the public and affected individuals about how AI systems arrive at particular decisions autonomously.[118] This would also include notification to individuals about the usage of personal data.[119]

The discussion highlights specific international instruments which have direct and indirect impacts on AI, especially in respect of corporate governance accountability, within the jurisdictional parameters of South Africa and the European Union. This includes both binding and non–binding instruments. Guidance will also be derived from soft law principles, playing critical role in shaping regulation and governance of AI systems.

Specific human rights regimes vulnerable to AI disruptions are also identified and examined as they may be affected by corporate governance decision making processes are evaluated.

Applicable international legal instruments and regulatory regimes relating to international trade and intellectual property law are also considered. The inextricable link between these areas of law makes it extremely important to address and bring into perspective within the context of corporate accountability.

An evaluation of the legal implications of AI systems is conducted with reference to selected international legal sources in the European Union. To understand the impact and challenges posed by AI, it is also important to examine some of the critical fundamental rights sacrosanct to the basic livelihood of humanity. Central to humanity's livelihood is the impact which

---

[117] A/HRC/43/29, para. 52, and A/73/348, para. 49.
[118] 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, para. 4.2.
[119] A/73/348, para. 49.

AIS has on the conduct of international trade and the global governance of intellectual property.

According to the European Union report, AI systems are fast-evolving family of technologies that can bring a wide range of economic and societal benefits across the entire spectrum of political, social - economic value chain.[120] The systems are regarded as instrumental in terms of improving prediction, optimising operations and resource allocation. The use of AI systems plays a critical role in supporting socio – economic spinoffs in improving the welfare of the people.[121]

3.2 International law instruments relevant to AIS

If the international community did not respond appropriately to nascent technologies during successive eras of industrial revolutions, the situation could have been more devastating to humanity. In addition, failure by the international community would have also rendered some international law and treaties irrelevant, due to failure to understand the intricacies and complexities of new technologies. In practical terms, a free reign to self-develop would imply abdicating international legal obligations to multi-national companies and technological innovations as they wish.

To a large extent, international law derives its existence from domestic legal rules informed by international custom, *jus cogens* as well as the creation of treaties. These international norms and rules come into being because of various factors such as political, military, socio-economic and demographic factors amongst others. A combination of these factors plays a role in the creation of international law. In general, these factors must be

---

[120] To this extent, on 21 April 2021 the European Union Parliament passed the Artificial Intelligence Act and Proposals for the Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (herein referred to as the Artificial Intelligence Act) and further amending certain Union legislative acts.

[121] Claudio Novelli C, Giorgio Bongiovanni & Giovanni Sartor, 'A Conceptual Framework for Legal Personality and its Application to Artificial Intelligence, Jurisprudence, DOI 2.

more forceful and compelling to warrant the international community to develop a law and ultimately legislate.

While there are no specific international instruments regulating AI, there are various sections of the Universal Declaration of Human Rights (UDHR) providing a solid base in addressing diverse societal concerns that have been raised around AI. The provisions include the right to equal protection in Article 2 and the concerns on the right to life and personal security provided for in Article 3.

Similarly, concerns around privacy due to the deployment of AI surveillance and algorithmic content moderation can be addressed in Article 12, while threats to freedom of expression is catered for in Article 19. The unjust treatment and displacement of human workers as well as the adequate standard of living following deployment of AI systems finds protection in Articles 23 and 25 respectively, as would be demonstrated below.

While domestic law is amended from time to time, international law changes over time. This has always been the case with the emergence of the 1st, 2nd and 3rd Industrial Revolutions. It is therefore not surprising that the 4th Industrial Revolution has emerged with unprecedented advanced technological innovations one of which is the Artificial Intelligence systems.

Following the 1995 European Union Data Protection Directive, the European Union adopted General Data Protection Regulation (GDPR) in 2016 as a primary instrument regulating challenges brought about by data collection and technological and socioeconomic reforms. The regulations are also underpinned by principles that guarantee fundamental rights and ensure people have some form of control over their personal data.

The GDPR binds all member states and all public institutions and companies operating within the EU jurisdiction.[122] However, the regulations and rules apply if the processing of personal data is involved. The exception is when such data is used for prevention, detection, or investigation purposes in offenses that are inherently criminal.[123]Regarding cross-border usage of personal data, the GDPR requires that such transfer should only take place if the transaction is consistent with EU privacy laws.

In 2020, the Court of Justice of the European Union (CJEU) handed a ruling in favour of an Austrian lawyer and privacy activist (Maximilian Schrems) declaring invalid the US – EU Privacy Shield Agreement, in a judgment popularly known as Schrems II. The Agreement in question relates to the transfer and commercialization of personal data from the European Economic Community to the US in compliance with data protection laws on both sides of the ocean. [124]

The dispute, in this case, emanates from the fact that a subscriber to the social media platform, Facebook, is required to enter into a contract with its parent company before they are admitted to the platform. [125] Mr. Schrems has been subscribing to Facebook since its inception in 2008. The contract in question makes it possible for the transfer of all or some of

---

[122] By 2019, Greece, Slovenia and Portugal had not yet ratified it. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data. (15 September 2023).

[123] Paloma Kroot Tupay, Martin Ebers, Jakob Juksaar & Kea Kohv, Is European Data Protection Toxic for Innovative AI? An Estonia Perspective (2021) 30 Juridica International 99. https://0-ww-heinonline-org.ultmillen.ul.ac.za/HOL/Page?public=true&handle=hein.journals/jurdint30&div=16&start_page=99&collection=journals&set_as_cursor=42&men_tab=srchresults. (15 September 2022).

[124] Maximillian Schrems v Data Protection Commissioner) 21 July 2000, the European Commission's Decision 2000/520/EC of 26 July 2020) in October 2020. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems | European Data Protection Board (europa.eu)_.(15 September 2023).

[125] Schrems 50.

the personal data of any person within the EU to Facebook servers that are located at its headquarters in the US, where further processing also takes place. In the light of this, Mr. Schrems lodged an application with the Commissioner demanding the prohibition of transfers of his personal data to the US amongst others.

He argued that the US law and practice do not provide for adequate protection against surveillance activities in line with the provisions of Article 3 (2) of Directive 95/46 issued under the GDPR.[126] The court noted that while the US has several security laws, these laws have shortcomings thus providing no adequate protection to data subjects. The court found that the decisions of the Ombud established in terms of the Privacy Shield Agreement are not binding on the US intelligence services.

Against this backdrop, the court ruled that communication of personal data to a third party, the US in this case, constitutes an interference with privacy rights as provided for in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[127] The court further held that the retention and access to such personal data and its usage by public authorities also interfere with these rights, regardless of whether the information is sensitive or inconvenient to the data subject.

Against this backdrop, the European Commission has now moved swiftly to develop and introduce a concrete legal framework as part of the proposal for the regulation of AI in 2020. This culminated with the introduction of the European Union Act on Artificial Intelligence in 2021. The Act provides for the regulations and harmonization rules on artificial

---

[126] Schrems 52.

[127] Schrems 171. Articles 7 and 8 of the Charter empowers the Commission to ensure that a particular level of protection afforded, known as adequacy decision, in accordance with the European Union. In practical terms, Article 7 of the Charter states that “everyone has the right to respect for his or her private and family life, home and communications. Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her”.

intelligence through mandatory requirements and prohibitory measures within the Union jurisdiction.[128] Amongst others, the regulations clearly define AI, identifies associated risks and compliance measures, and further sets out monitoring and enforcement mechanisms. The relevant provisions of the Act are fully discussed in the subsequent study chapter.

In addition, the relevant instrument in terms of police and security operations, the EU has adopted a Law Enforcement Directive (Directive (EU) 2016/68021), which establishes a comprehensive system of personal data protection for biometric matching, identification and authentication of persons of interest. This is mainly used in cases of terrorism, migration e sectorial EU instruments governing large-scale EU information systems in the field of migration and security.[129] Biometric data is defined as in the EU Directive as the:[130]

> "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy [fingerprint] data."

The EU data protection law recognizes physical and physiological characteristics as biometric data. The physical characteristics relate to facial features, fingerprints, retina, and iris of the eye, while physiological ones include personality traits, actions, deeply ingrained habits, and addictions amongst others.[131]

---

[128] Regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 2021 COM (2021) 206.
[129] Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).
[130] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 as amended by Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89 (Law Enforcement Directive), OJ L 119, 4.5.2016, pp. 89-131.
[131] Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

One of the dire consequences of biometric data collection, through AIS, is that it would disadvantage vulnerable groups such as children and elder persons, in that their facial and physical appearance changes with age from time to time. This has the potential to disadvantage these social groups when it comes to access and benefits to public and private services.

The discussion that follows identifies and unpacks international instruments relevant to and impacting on AI. These are a non – exhaustive legal instruments at the disposal of our courts and other regulatory bodies that can be used to hold accountable corporate companies and other business entities. In identifying international instruments regulating AI, the discussion also applies the instruments to given set of cases handled by the courts and other regulatory bodies in the EU and South Africa to hold corporate companies accountable and liable.

3. 3 Protection of the right to life and security

The use and deployment if AIS may result in breach of both negative and positive obligations relating to the right to life and security, especially in areas of criminal justice system, environmental pollution, and health amongst others. At the centre of production, manufacturing and deployment of these systems is corporate private enterprises with governments playing a limited role.

In most cases, public authorities and corporate companies procure these tools from private vendors, systems developers and suppliers. By using data analytics and design choices to code policy choices, engineers at these vendors plays a critical role in influencing decisions in both the corporate world and public sector. In a way, governments have literally abdicated its decision – making responsibilities to private entities by using and deploying these tools. It means that unmandated and unelected

officials and entities are in a position to influence decisions by public authorities. While artificial intelligence provide support for enjoyment of life and related rights, conversely it can also have an adverse effect on these rights. This support can be in the form of diagnosis and treatment of medical conditions. In the medical practice, AIS are used to carry out medical procedures and surgery and possibility exist that some of these equipment may be faulty or even malfunction in the process, thus posing a threat to the right to life, liberty and security of a person.

An example of this would relate to medical diagnosis in radiology which uses image analysis systems for mammogram. In a research carried out by Zhou et al., a generative adversarial network (deep learning models) model was used to modify or fake images that would detect breast cancer.[132] After the modified images were analysed by AIS and radiologists, the adversarial samples analysed by AI gave a wrong diagnosis at 69% while images analysed by radiologists identified between 29% - 71%.[133] This means that that a wrong cancer diagnosis may result in a wrong prescription for medication and ultimately resulting in serious risks to the right to life and health.

The right to life and security of a person is one of the fundamental rights provided for in Article 9 of the International Convention on Civil and Political Rights. The Article provides everyone has the right to life, liberty, and security and that no one shall be subjected to arbitrary arrest, detention, or sentenced to death. The convention is clear that the right to life is inherent to a human being and as such, no one shall be arbitrarily deprived of this right contrary to the procedure established by law.

---

[132] Zhou, Q., Zuley, M., Guo, Y. *et al.* A machine and human reader study on AI diagnosis model safety under attacks of adversarial images. National Communication 12, 7281 (2021). < https://www.nature.com/articles/s41467-021-27577-x.pdf?pdf=button%20sticky. (24 December 2022).
[133] Zhou et al 6.

While some countries still impose a death sentence, the Convention asserts that such sentences can only be imposed in exceptional circumstances and following applicable law in force and should not be contrary to the provisions laid out in Article 6.

The mere fact that one's online personal data can be accessed at a whim by authorities for any reason poses a threat to the right to life and personal security. State agents can easily use this to deal with detractors currently or in the not-so-distant future. However, the courts in the EU have been reluctant to grant standing, especially in cases involving data breaches.

3. 4 The right to equality and protection from discrimination

The right to equality is rooted in century-old struggles against slavery, colonialism, and racism which have spanned from the Stone Age up until now. Algorithmic discrimination and racial bias have been documented as we enter the transition from the 3IR to the 4IR driven by the deployment of AI. The mannerism of data collection and their orientation remains a fertile ground posing a threat to this right.

In all circumstances, discrimination risks must be prevented and mitigated with special attention for groups that have an increased risk of their rights being disproportionately impacted by AI. This includes women, children, older people, racial and minority groupings, and members of the LGBTI community amongst others. Member states must refrain from using AI systems that discriminate or lead to discriminatory outcomes and, within their jurisdiction, protect individuals from the consequences of use of such AI systems by third parties.

Equality as a right is guaranteed in Article 9 of the UN Charter on Human Rights. The right to equality is an inalienable right guaranteed in many regional and national instruments in different jurisdictions. In determining criminal charges under any law, a person is entitled to a fair and public

hearing by an independent and impartial tribunal without any biases and prejudice. To this end, Article 2(1) of the International Covenant on Civil and Political Rights prohibits discrimination of any form expressly and provides thus:[134]

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or another opinion, national or social origin, property, birth or another status.

In the EU, equality rights and protection from discrimination are protected under Article 14 of the European Convention on Human Rights (ECHR) and accompanying Protocol 2. The provisions are aimed at prohibiting categorizations of AI systems based on new differentiations that may give rise to discriminatory stereotypes.[135]

Article 4(1) of the newly adopted EU Employment Equality Directive provides for differential treatment on discrimination–relevant grounds such as sex. This is on the proviso that such treatment shall not constitute discrimination and further be able to meet occupational requirements that are legitimate, justifiable, and proportionate. This is problematic because it throws into open what discrimination means in this context. This is because the link between activity, context, and personal trait is factual as they include normative assumptions about appropriateness and reasonableness.

In grappling with a similar matter relating to recruitment in churches, the European Court of Justice restricted this kind of approach.[136] The court

---

[134] The International Covenant on Civil and Political Rights was adopted by the UN General Assembly in December 1966.

[135] Council of Europe (2020) Preventing discrimination caused by the use of artificial intelligence. https://ennhri.org/about-nhris/human-rights-based-approach/. (20 June 2022).

decided that a genuine, legitimate, and justified occupational requirement is necessary and resonates with the provisions in Article 4(2). The court further ruled that the occupational requirement justifications should comply with the principle of proportionality, guided by the nature of the occupational activity as well as moral and ethical consideration of the religious institution concerned.[137] In practical terms, this means that religious institutions cannot be allowed to reject job applicants suspected of having divergent religious beliefs, for example.

3. 5 The presumption of innocent and fair trial rights

Increasingly, while various levels of public authorities deploy AI systems to administer the criminal justice systems for efficiency and effectiveness, elements of bias within these systems are concerning. These AI systems are mostly acquired and procured from private vendors. There have been admissions that the databases and algorithm collected and fed into the AI systems reinforces and entrench bias within the criminal justice systems as opposed to its elimination.

It is for these reasons that an accused person may challenge the usage and outcomes of AIS used in investigative processes of alleged crime. Critical to this is the possibility of the accused in inspecting and testing the computational components and accuracy of algorithm underpinning the AI systems. Through defence counsel, the accused must be able to challenge, and review raise questions relating to reliability and accuracy of these systems, included embedded bias.

The defence team should be entitled to have access to observe and inspect how the black box and source codes arrived at the emergent

---

[136] The European Court of Justice (case C-414/16 as of 17 April 2018). < http://www.europeanrights.eu/public/commenti/BRONZINI14-CONTRIBUTO_GORI_NEWSLETTER_DICEMBRE-11_-_Charter_-_Vera_Egenberger_-_Gori.pdf. (21 June 2022).

[137] Ibid.

results to resulted in negative findings against the accused, especially taking into account its opaque nature. According to Reyes, those concerned with access to information about AI systems in order to assist in a proper defence emphasize that due process requires transparency, including a notice and the opportunity to challenge.[138]

In resolving AI problems threatening fair trial rights in the criminal justice systems, issues of accountability, transparency and fairness must be prioritized and attended to. For this reason, it should be obligatory for creators and producers of AI systems to ensure biased data is not used in order to comply with fairness requirements.

The availability and unfettered access to personal data by corporate companies especially on social media platforms may be used by law enforcement agencies in the future and this is likely to influence prosecutorial and judicial decisions by the courts. The deployment of machine learning tools is susceptible to harnessing and identifying a person's language and behaviour as having a risk propensity to commit certain crimes. As a result, the deployment of AI systems may have dire implications on the right to be presumed innocent as provided for in Article 14 of the ICCPR.

The increasing usage of risk–scoring software based on AI has been proven to be interfering with the right to personal liberty. This software is used to inform decisions around detention and bail applications in criminal matters.[139] It has been proven that this has resulted in more suspects of African origin being falsely categorized and labelled as high risk with the

---

[138] Reyes, Carla, Emerging Technology's Language Wars: AI and Criminal Justice (2022). Journal of Law & Innovation (2022 Forthcoming), SMU Dedman School of Law Legal Studies Research Paper No. 568, Available at SSRN: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217020 (02 June 2022).

[139] Maya C. Jackson, Artificial Intelligence & Algorithmic Bias: The Issues with Technology Reflecting History & Humans, 16 J. Bus. & Tech. L. 299 (2021). < https://digitalcommons.law.umaryland.edu/jbtl/vol16/iss2/5. (18 June 2022).

possibility of ordering stringent bail conditions or receiving longer prison terms if convicted by the courts.

Where predictive policing software is used, potential risks exist that guilt can be wrongly imputed to persons as a result of built-in police biases based on previous data. The possibility exists that such inbuild biases may emanate from the moment an AI device is manufactured and produced because the device itself learns from the sociological make–up of the person who inputted the algorithm and coding. In the US and UK, there have been reports to the effect that some judges rely heavily on software results without a clear understanding of the risk - scoring system works.[140]

It is therefore clear that court decisions arrived at based on risk–scoring systems by the software are inherently unfair. To a particular extent, it also shows that the judiciary has capitulated its judicial powers to private vendors and engineers who even lack the titles to prosecute court cases.

A study conducted by the European Court of Human Rights has revealed that, on average, there is accurate prediction of 75% of violation of nine articles of the European Convention on Human Rights.[141] This is not surprising since Article 8 of the European Union Charter on Fundamental Rights recognize the potential for AI to create and reinforce bias and provides that:

> 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 the law.

---

[140] The software is AI-powered and produced by tech companies, most of which are owned by conservative companies.

[141] Masha Medvedeva, Michel Vols and Martijn Wieling, Judicial Decisions of the European Court of Human Rights: Looking into the Crystal Ball (A Paper delivered at a Conference on Empirical Legal Studies in Europe, 31 May – 1 June 2018). (19 June 2023).

It is possible that in future, it may be difficult to plead self – defence especially in cases of car accidents at robot intersections. This could be the case because of the inability of AI to deal with the question of nuances. Is it acceptable and justifiable in law to jump a red robot to evade an imminent accident and save a life? While a law enforcement official on duty witnessing the incident may be understanding and not issue a ticket, an AI-powered robot may act on this and issue a traffic violation ticket issued on the spot. Arguably, it can be concluded that there is a potential risk that the loss of nuances by AI-powered tools in situations like this could have far-reaching implications where extenuating circumstances exist.

3. 6 Freedom of movement and usage of surveillance tools

The continued development and deployment of information and communication technologies to generate evidence have equally resulted in the generation of new forms of crime. These forms of technology have been embedded with AIS to enhance and support law enforcement agencies in the fight against crime through prevention, detection, investigations, prosecution, and enforcement.

As a result, close–circuit televisions (CCTV) are prominently placed in strategic centres in smart cities to assist in this regard. However, evidence obtained from devices requires care to ensure its authenticity and integrity remain intact as it may be easily manipulated, modified, deleted, or even overwritten to conceal evidence.

In some instances, this may result in a deepfake where AIS is used to superimpose images or videos of a person onto the body of someone else to create a digital lookalike. The proliferation of deepfakes has presented challenges to the courts in assessing the authenticity of such images. While an independent expert may verify such evidence, it could still leave

doubts on interested parties thus prolonging proceedings before the courts. Deepfake manifests itself in acts that encroach on privacy rights, harassment, defamation cases, and intellectual property laws.[142]

Article 12 of the ICCPR provides for the freedom of movement and the right to choose own residence, provided it is necessary to safeguard national security, public order, and public health. These rights cannot be arbitrarily deprived.

Amongst others, the use of surveillance tools based on AI involves combining data from satellite images through facial recognition cameras and cell phones, the Live Facial Recognition Technology. This provides detailed information about a person's movement and in the process predicts future movements.

It is possible that GPS mapping will be installed and extended to communities that are not currently covered around the world as part of predictive policing in smart cities and along the highways. In this regard, an automated decision can be made that one is a flight risk in a travel list in real-time. This would prove to be an impairment of the freedom of movement and other connected rights such as tourism amongst others despite legitimate intentions for public safety and security.

In R v Chief Constable of Wales Police, the accused alleged that facial recognition technology was used to monitor him on two occasions. This resulted in the violation his freedoms and privacy rights in contravention of Article 8 of the European Convention on Human Rights.[143] The provision of

---

[142] Delfino, Rebecca, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act (February 25, 2019). 88 Fordham L. Rev. Vol. 887 (December 2019), Loyola Law School, Los Angeles Legal Studies Research Paper No. 201908.SSRN: https://ssrn.com/abstract=3341593 or http://dx.doi.org/10.2139/ssrn.3341593. (11 January 2023).

[143] R (on the application of Edward Bridges) v Chief Constable of South Wales Police (Respondent) and Secretary of State for the Home Department and the Information

the Article requires that such facial recognition technology must be used in consistent with the law.

The technology in question uses biometrics and other unique biological data obtained from a database of pictures collected indiscriminately in various ways. The technology was used as a pilot project to identify wanted and suspected persons in large crowds.

In this case, a decision of the lower court was overturned by the Court of Appeal, which ruled that the deployment of these tools contravened EU law relating to privacy. The court found that the technology used violated the right to privacy and freedom of movement guaranteed in Article 8, which requires the interference to be in accordance with the law.

Similarly, freedom of movement and data privacy can be curtailed even in the workplace. In this regard, the critical question to ask is whether employers can monitor employees when they work from home. Following the imposition of a state of disaster in the wake of Covid 19, numerous employers deployed IAS to monitor employees' productivity working from home. Depending on the AIS embedded on the app, monitoring can be conducted in various forms such as the opening of emails; checking online behaviour such as time spent on work-related apps; tracking websites visited; taking screenshots of what was typed on those websites; physical location tracking and, even, webcam surveillance and taking photos of employees whilst they are working.

Depending on the legislative framework obtaining in a particular jurisdiction, the legality of employee monitoring using AI systems is debatable. While it may be accepted under a particular jurisdiction, it is bound to be subject to particular safeguards such as prior notice which

---

Commissioner, the Surveillance Camera Commissioner, and the Police and Crime Commissioner for South Wales (Interested Parties) [2020] EWCA Civ 1058.

may be provided for in another jurisdiction. Yet, even if those safeguards are met, the practice of working from home was never envisaged. Under the circumstances, broader questions of human rights law would then come into the picture. The fundamental question being whether the monitoring can be regarded as a justifiable limitation of employees' reasonable expectation of privacy while working within the confines of their homes.

In the most recent case, a Dutch District court dealt with a matter where an employee was dismissed for refusing to comply with the employer's instruction to leave the webcam on the camera throughout working hours.[144] A US-based software development company, Chetu Inc[145], employed a telemarketer in the Netherlands and demanded that for the first 90 days of employment, the employee was required to log on, share screen, and leave his computer screen on. However, the company insisted this to continue even after the completion of the probation period by the employee.

In court, the employee argued that the flighting of webcam throughout the working hours make it uncomfortable and this violates privacy rights. The employee further argued that the company already uses share screening function on the laptop to monitor work performance. The employer argued that by doing that, the employee refused to work, and as such this amounted to insubordination.

The court found that the dismissal was invalid due to insufficient refusal to work. It also found that the instruction to have the webcam all working hours violated the employee's right to respect for private life and as such

[144]ECLI:NL:RBZWB:2022:5656 - District Court Zeeland-West-Brabant, 28-09-2022 / 10072897 AZ VERZ 22-61 <Rechtbank Zeeland-West-Brabant 28 September 2022, ECLI:NL:RBZWB:2022:5656 (18 June 2022)

[145] Chetu, Inc.Vko Gaming, Inc., 261 So. 3d 605 (2019) January. District Court of Appeal of Florida. No.4D18 – 1551. <Chetu, Inc. v. KO Gaming, Inc., 261 So. 3d 605 (2019) | Caselaw Access Project. (28 June 2022).

unreasonable. The court observed that video surveillance of employees, both covert and overt, is subject to strict conditions and is regarded as a considerable intrusion of employee's private life resulting in the violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The court held that:

> 'any interference with this right may only be justified if it is in accordance with the law, pursues one or more of the legitimate aims to which that provision refers and is necessary in a democratic society in order to achieve any such aim.[146]

The court further asserted that while, in principle, the fundamental right enshrined in Article 8 directly applies between states and citizens, it can also be applied vertically in a private-law employment relationship under certain circumstances.[147] These circumstances may relate to when a state does not sufficiently offer protection of a fundamental right in question. For these reasons, it ruled that the employee must be reinstated and compensated for lost salary and other benefits due to the employee. In addition, the court imposed a fine on the company in question.[148]

That as it may, as indicated above various concerns have been raised on the opacity of most of these AI systems. The concerns are based on the fact that prediction models used by AI systems have demonstrated that these neutral systems are susceptible to replicate biases. These biases are inherent in the data and codes they are trained on thus mimicking the psychological and mental disposition of a person who fed algorithm databases. Therefore, corporate companies and other service providers involved in producing and trading these AI systems would have to be held accountable, jointly and severally guided by existing legislative framework as it would be shown in the next chapter.

---

[146] Article 8 (2) of the Convention.
[147] Chetu Incorporated 4.7.
[148] Chetu Incorporated 4.2.

3. 7 Privacy rights and data protection

The development, training, testing, and use of AI systems that rely on the processing of personal data must fully secure a person's right to respect for private and family life, including the right to self-determination in relation to their data.

Privacy rights are protected under Article 12 of the UN Declaration of Human Rights and 17 of the ICCPR, which affords protection to 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 Charter of Fundamental Rights, which guarantees the protection of the right to personal data. The provisions further require consent as a pre – condition for before a personal data can be fairly processed for a legitimate purpose.

In this way, privacy is viewed as a fundamental right essential to human security and comfort. The right 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 as part of it within the UN human rights system. It is for this reason that most governments in the EU are now recognizing the right to data protection.

Title IV of the AI Regulations imposes certain transparency obligations for corporate companies to comply with. These obligations include that a person must be informed when their character or emotions interact with an AI system, such as a chatbot. 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 in this case.

Most significantly, AI systems are trained using 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 to accurately estimate personal data by merely using their previous and future location on their cell phone, including those of their close associates.[149] It is then clear that most of these personal details are protected information that must be treated with all sensitivity and respect for the person concerned.

In the EU, the European Court on Huma Rights dealt with the requirement of foreseeability when surveillance measures are used in the interception of communication in the *Liberty* case.[150] The surveillance measures were used to monitor a person through filtering techniques. The techniques were consisting of automated sorting systems which selected keywords from a technical database.[151]

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 to intercept and examine external communications by the state.[152] The reason for this relates to fragmented legislation in the EU on this aspect. The current proposals seeks to harmonise regulations in the Union jurisdiction

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. For this reason, it was ruled that the interference with applicants' rights could not be regarded as violating Article 8 of the ECHR.

---

[149] Steven M. Bellovin, et. al, "When enough is enough: Location tracking, mosaic theory, and machine learning," NYU Journal of Law and Liberty, 8(2) (2014) 555—628. < https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2379&context=fac_pubs. (Accessed 25 August 2022).
[150] Liberty & Others v the United Kingdom, judgment 1 July 2008.
[151] Liberty 43.
[152] Liberty 69.

Amongst others, notification to concerned individuals should always be at the fore, though it should not necessarily take place during surveillance but afterward, to not defeat the object of surveillance. Therefore, the court viewed notification as being inextricably linked to the safeguard against abuse of surveillance measures that are intrusive to privacy rights.[153]

3. 8 Vulnerable platform workers and the right to work

State parties are obliged to work towards a full realization of the right to work and adequate living standards in line with the provisions of Article 6 and 11 of the International Convention on Economic, Social, and Cultural Rights. There is a recognition by these 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, state 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 AIS at the workplace poses a serious challenge to constitutionally protected right to work, especially to vulnerable platform workers whose rights are violated and 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 bears different names, business models, and playing different roles vacillating along labour brokers, outsourcing and intermediaries based on labour demand and supply. Most of these workers only interact or work from home or work as telemarketers for various apps and platforms which are AI driven. According to Rasioru, this has become a common practice in Romania where different digital

[153] Weber and Saravia v. Germany, 29 June 2006, paragraph 135.

platforms and app circumvent existing labour laws to manipulate desperate workers.[154]

Most public sector entities and companies procure AI systems from various specialist tech companies for the purposes of advertisement, recruitment, performance management, and payroll management systems among others. It is possible that machine–learning algorithms used by these third-party companies may reinforce human prejudices targeting unsuspecting employees. This may result in unscrupulous advertising companies using algorithms targeting people with low income to generate high-interest loans, for example.

The world all over, employment laws are geared at preventing discrimination based on the grounds of race, sex, religion, disability and age amongst others. In evaluating individual employees for possible employment or promotion, AIS is 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 would result in massive job losses and unemployment resulting in the infringement of the right to work and ultimately the right to adequate living standard. Throughout the world, the automation of workplace operations has already resulted in shedding of jobs in certain economic sectors. It would seem that this trend would continue to rise with time. Conversely, there is consensus that effective use of AI would also yield more jobs as compared to job destruction given expected shifts in the labour market.

The utilization of software for background screening has also raised concerns not only about the possible perpetuation of discriminatory practices against potential employees, but also about organisational rights

[154] Felicia 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. (29 June 2022.)

at the workplace. The emergence of the novel coronavirus has forced my companies to fall back on home - based remote working, using technological tools of trade linked to company servers. This has significantly resulted in union bashing and limited employee's right to assemble, protest, and bargain especially considering the loss of benefits by employees as a result of lockdown regulations throughout the world.[155]

In the midst of this, Data Protection Authorities declared invalid the use of fingerprints at the workplace as part of clocking system in Italy[156] and Greece[157]. This was because such systems utilizes AIS which infringes the right to privacy, dignity and personal data. The basis of these decisions is that such purpose can still be attained by using other, less privacy-intrusive systems, which do not impinge on privacy and do not involve an employee's body.

The usage 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 objective liability of the owner coupled with European product liability.

Germany is one of the first EU state to formally adopt a legal framework for allowing the user of a vehicle to disengage from driving completely.[158]

---

[155] 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 the workers would be in a weaker position. <200805_Union_busting_unfair_dismissals_garment_workers_during_COVID19.pdf (business-humanrights.org). (28 September 2022).

[156] The Garante per la protezione dei dati personali, Provision of July 21, 2005.

[157] The Greek Data Protection Authority, Decision of 20/3/2000.

[158] The Law of 11 June 2017, the Federal Law Gazette, Amending the Road Traffic Act, as announced on 5 March 2003 (Federal Law Gazette page 310, 919). Gresley,

The legislation also imposes a ban on non–passenger driving systems, save for low-speed parking systems only on private grounds.[159] The legislation further prescribes that the designing of these vehicles should have proper space and time to allow transitioning from automated system to human driver system to ensure there is control. It is also obligatory for manufacturers to install electronic units and black boxes in vehicles, which 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 cases of claims for product liability.

3. 9 Potential international trade barriers and the right to trade

Apart from the World Bank and International Monetary Fund (IMF), the World Trade Organisation (WTO) was formally established by the Marrakesh Agreement in 1995. This was after more than fifty years of negotiations by mostly powerful countries and transnational corporations, with South Africa being one of the founding members.[160] The WTO is charged with the responsibility of managing and regulating international trade.

The rules used by the WTO to conduct international trade include both General Agreement on Tariffs and Trade (GATT) and Trade-Related Intellectual Property Measures (TRIPS Agreement). While the WTO is not

---

Jenny. *Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads*. 2021. Web Page. https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/. (30 June 2022).

[159] *European Journal of Law and Economics* (2021) 51:243–284 <https://doi.org/10.1007/s10657-020-09671-5. (30 June 2022).

[160] The World Trade Organization was formally established in terms of Article 1 of the WTO Agreement, registered under Article 102 of the UN Charter. In terms of the WTO Agreement, no reservations may be made upon signing it and will only be allowed in terms applicable to the Agreement itself.

an agency of the UN, the two have maintained strong relations in line with the provisions of Article 102 of the UN Charter since 1995.[161] The WTO has as an independent entity whose accountability cannot be accounted for.

The emergence of the digital economy underpinned by AIS would require private and public sector authorities to embark on a series of trade negotiations to establish international legal framework, rules, and standards in the digital era. Since existing trade rules have significant shortcomings, they require to be updated to at least try to match the demands of the digital economy as it unfolds. In particular, there would be a need for new trade rules in areas of intellectual property protection for source codes, algorithms, and data protection amongst others.

It is evident that the high level of autonomy of AI systems and the possible emergence of AGI, in the long run, has resulted in public perception anthropomorphizing and humanizing even narrow AI systems. According to a Taiwanese legal scholar, Liu, in the end, this social valence tends to distort the thin line that exists between a 'thing' and 'humans.'[162] The critical question raised by Liu is whether these AIS should then be treated as tools, agents, or legal persons or even create a new ontological category in between for regulatory purposes. This is in light of the fact that more and more AIS becoming fully autonomous thus making legal and social consequences more indeterminate and complex.

It is against this backdrop that legal issues pertaining to international trade and freedom to trade arise. The WTO is underpinned by two main agreements, i.e., the General Agreement on Tariffs and Trade (GATT) and

---

[161] Arrangements for Effective Cooperation with other Intergovernmental Organizations < https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W10.pdf&Open=True. (15 September 2022).

[162] Liu, HW and Lin, CF, 2020. Artificial intelligence and global trade governance: a pluralist agenda. *Harvard International Law Journal 61,* 407. < https://harvardilj.org/wp-content/uploads/sites/15/61.2-Liu.pdf. (19 February 2023).

the General Agreement on Trade in Services (GATS).[163] The GATT applies to international trade in goods, while GATS regulates services. These international services relate to cross-border supply (including the movement of natural persons supplying services), consumption, and commercial presence. When some of these goods and services were identified and created, most of the existing e–commerce and digital products were not in place.

The emergence of digitization and usage of IAS by corporate companies exposes limitations underpinning international trade rules as expounded by the GATT and GATS axis. This bifurcated traditional way of conducting international trade in goods and services poses challenges of corporate legal accountability, especially in relation to intellectual property protection for source codes, algorithms, and data protection amongst others.

To operate effectively, international trade requires unfettered access to the massive global database to use AI systems productively. This will ensure that it responds to diverse challenges and different population groups critical for international trade. It is therefore imperative that such a database must be representative of diverse official languages, linguistic expressions and all commonly used words across borders. Otherwise, genuine efforts to develop tailored AI capacity will be reduced by failure to localize data collection.

Because cross-border data flows are critical, existing technologies would result in the development and use of AI systems much more effortless. Therefore, restrictions on global data transfers and collection will negatively impact data localization measures resulting in less data availability. Going forward, this may affect developing countries as witnessed during the search for Covid 19 vaccine.[164] Hopefully, data

[163] The Resource Book on TRIPS and Development: An Authoritative and practical guide to the TRIPS Agreement, UNCTAD-ICTSD, < https://unctad.org/system/files/official-document/ictsd2005d1_en.pdf. (15 September 2022).

collected during vaccination of coronavirus pandemic will become handy, provided it will be used for good causes. A debate for another day.

It would seem like some western countries are reluctant to commit to free cross-border data flow on trade agreements on account of domestic public policy bordering on privacy standards. The apparent lack of transparency in decision-making within the WTO should be a cause for concern, especially in the developing world. What is also disturbing is the fact that it is unclear to which international institution would hold the WTO accountable, if it runs roughshod over existing rules involving AI systems and their deployment.

3. 10 Implication for AI generated intellectual property rights

Copyright relates to entitlements to property rights subsisting in various intellectual works. These works included sound recordings, films, and literary works amongst others. Copyright entitles the bearer to the right to do certain things which cannot be copied or broadcast without due consent. Anyone infringing on this right may be subject to legal action. It is therefore within this context that ownership of a copyright is inalienable but can be transferred to another who will be permitted to do specified acts.

In discussing copyright, the point of departure is the definition of authorship of copyrighted works. According to Locke's natural right theory, the intellectual labour of an author justifies the author's right over the fruit of their labour.

However, the picture becomes different when a copyrighted article is owned by a non -a human entity like an AI system. In the absence of clear

---

[164] Jana Subramanian, Challenges in Cross Border Data Flows and Data Localization amidst new Regulations, SAP Africa Report Blog,19 January 2022. Challenges in Cross Border Data Flows and Data Localization amidst new Regulations | SAP Blogs. (16 September 2022).

legal frameworks, the courts have come on board to provide guidance. It is in this context that the definition of authorship in the light of the 4IR propelled by AI becomes critical.

Lack of clarity on the legal status of AI poses questions about the assumption of authorship as well as whether an AI system can indeed create own and exercise copyright over an article independently. This is because it is not clear as to whether copyright should belong to a developer or a customer company who uses it on the one hand, or the AI itself as a legal person on the other hand.

International copyright law revolves around three key international treaties, namely the Berne Convention, the WIPO Copyright Treaty, and TRIPS Agreement.[165] While the UN system has some modicum of control in these institutions, the World Trade Organisation wields unbridled authority over them.

The EU and majority of its Union members subscribes to all the treaties discussed so far. From the inception of the Berne Convention in 1886 until the adoption of the Agreement on Trade-Related Aspects of Intellectual Property Rights in 1995[166], the concept of intellectual property has been able to evolve and adapt to new technological innovations to protect and encourage creativity and entrepreneurship.

3.10.1 The presumption of authorship in the EU

[165] These include Berne Convention for the Protection of Literary and Artistic Works as amended on September 28, 1979, the World Intellectual Property Organisation Copyright Treaty (WIPO), and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs).

[166] Therefore, Article 7 of the TRIPS Agreement does allow for the protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation as well as the transfer and dissemination of technology. This should be for the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

Authorship as a concept is indirectly referred to in Article 15 of Berne Convention, which stipulates that if the author's name is indicated on copyright application, the name of the person appearing on the article shall be regarded as the author of a literary or artistic work in the absence of contrary proof. While the provision does not define what the author means, it offers some degree of certainty by reducing the burden of proof required. This is where the question of authorship arises, especially when the name of either a natural or juristic person is mentioned in the works. Contrary to provisions in the Convention, both the WIPO and TRIPS Agreement are silent in defining authorship. In a way, this provides state parties a discretion to work out their diversified approach on what exactly the concept of authorship in copyright entails amongst others.

It is for these reasons that in an attempt to harmonize these interlocking diversities, the EU adopted the Computer Program Directives in respect of cinematographic and audio–visual works. Article 2 (1) of the Directives stipulates that that the author of a computer program shall be a natural person or group of natural persons who have created the program. Alternatively, the author must be a legal person designated as the right holder by a legislation.[167] There are two meanings that could be inferred from these provisions. First, the general principle is that a natural person or a human being is identified as an author who conceived and created the computer program. Secondly, references to a right holder could include an author or any other person outside a legal person.

To further cement an understanding of the meaning of authorship as a natural person, Article 2(2) of the Rental and Lending Directive as well as Article 1(5) of the Satellite Directive uses the concept of a director to designate an author of cinematographic and audio-visual works.

[164] The Directive of The European Parliament And The Council on The Protection of Computer Programmes, 23 April 2009, [2009] OJ L111.

Unfortunately, the problem is that definition of authorship in these provisions is made about specific works except for AI-inspired ones.

3.10.2 Guidance provided by the regulatory regimes in the EU

The relevant legislative framework which has proven helpful in defining authorship within the context of algorithmic authorship is the Copyright Designs and Patents Act of 1988. Section 11 (1) of the Act provides that an author of a work is the first owner of any copyright, subject to certain exceptions not relevant here. Section 9 (1) goes further to provide that an author, in relation to a work, means the person who created such work. It is therefore from these provisions that reference to an author directly means a human being.

However, the provisions in S 9(3) inspire a glimmer of hope towards recognizing algorithmic authorship. By defining authorship in relation to computer-generated works of literary, dramatic, musical, or artistic nature, the section makes a provision to the effect that, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken. Further than this, computer-generated works are also defined in section 178 to mean that such works are generated by a computer program in circumstances involving no human author.

The provisions in section 9 (3) seem to be anticipating that a computer or other machines could be developed which will create work without human intervention, following the arrangement of computer hardware and software by a human. However, the fact that the author has to be a person demonstrates that AI machines still cannot be clothed with an authorship title required to own a copyright in the UK in terms of these provisions.

There are different approaches within the EU member states and shows that harmonization is yet to be achieved in relation to authorship on intellectual property. For instance, Article 5 of the Spanish copyright law

expressly states that the author of a copyright-protected work is a natural person. The German copyright legislation in Article 7, provides that an author is the creator of the work and goes further to imply of an expected author is a natural person in a position to protect their intellectual property and personal relationship to the work.

The situation is interestingly different in the case of copyright law *(Tekijänoikeuslaki)* in Finland, where the nature of the author is not defined other than being a creator of the artistic works. Significantly, its Copyright Act deems an entity whose name or pseudonym appears on the works as the author. While there is no strong indication that an author is a natural person, there is no express mention to this effect in the Finnish legislative framework.[168]

Due to this fragmented approach, the current Proposal on the regulation of AI various mechanisms and processes have been put in place to harmonize the legislative framework in the EU. This matter is addressed in a subsequent chapter.

3.10.3 Inventorship and AI in the EU

In terms of Article 81 of the European Patent Convention, it is required that applications for patents should designate a natural person as an inventor. Alternatively, there must be an attachment of a statement outlining the origin of the right to a European patent if the applicant is not an inventor or a sole inventor. Another requirement is that a right to a European patent belongs to an inventor or his successor in title as provided for in Article 60 (1) of the Convention. The details which must be included in the application includes family names, names, residential addresses, and

[168] Koskela, A., Legal Framework of Copyright in Relation to the Development of Artificial Intell10gence. <https://digikogu.taltech.ee/en/Download/154c619f-f75f-4b44-bd45-b4a0e0ca02ef/Tehisintellektiarendamisegaseotudautoriiguste.pdf. (20 September 2022).

signatures in line with the formal requirements provided for in Article 81 read with Rule 19 of the European Patent Convention.

In an interesting recent ruling, the European Patent Office decline to recognize food processing container invented by an AI system. This is a food container consisting of fractal surface enhancing insulation and stacking. It also uses a flashlight in emergency cases to alert anyone who cares.

The question before the European Patent Office was whether Mr. Thaler, as the applicant for a patent can designate the AI machine, known as DABUS (Device for the Autonomous Bootstrapping of Unified Sentience), as the inventor.[169] Apart from the European Patent Office, the application was filed in various jurisdictions including the UK, US, Australia, and South Africa simultaneously (The Australian and South African rulings which recognized it will be discussed in subsequent chapters).

In describing DABUS as the inventor, the applicant initially characterized it as a connectionist artificial intelligence system from which he had acquired the right to the European patent as the employer. This was later changed to the effect that the applicant is a successor in title and that the invention was made by the machine using its own idea of novelty before a natural person came into the picture.

For these reasons, the applicant argued that the machine should therefore be recognized as the inventor while its owner should be regarded as an assignee of its intellectual property rights. The applicant maintained that this is in accordance with the objective of the EU patent system which aims to incentivize the disclosure of information, commercialization, and innovative inventions. In this regard, the applicant argued that

[169] European Patents Office, Applications number EP 18 275 163 and EP 18 275, 174 < https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false. (05 August 2022).

acknowledging machines as inventors would facilitate the protection of moral rights of human inventors and allow for recognition of the work of the machine's creators.

Regarding the requirements in Rule 19 (1), the applicant argued that the requirements to disclose names and family names would deny mononymous persons the right to be designated and named as inventors. In motivating DABUS as the actual devisor of the invention, the applicant invoked the fundamental principle underpinning patent law in section 7 (3) of the UK Patents Act which requires an indication of an actual devisor of an invention.

To this end, naming a person who is not the inventor of an invention undermines this principle and may constitute an offence. In essence, it would be in the public interest to disclose the actual inventor of the invention in question.

Another argument advanced was that because inventorship is determined before any rights, this cannot prevent the recognition of an inventor. This argument sought to point out that the rights of an invention are conferred to an inventor or successor in title, with ownership passing to the applicant (Mr. Thaler) as the owner of DABUS.

The EPO reasoned that naming things may not be equated with the names of natural persons, names given to natural persons are critical in identifying their personalities so that they are able to exercise their rights. It is for these reasons that the EPC recognizes only natural persons, legal persons, and other bodies acting in certain capacities. It was indicated that the legal framework in the EU is unambiguous that an inventor is a natural person.

It would seem like EPO missed the point here. According to Thaldar et al, this argument assumes that the inventor must always be able to be the

bearer of rights. He paints a situation where a person dies while their patent application is still being considered by the patent office and the right to the invention is ultimately granted to the deceased estate, which is not a legal person. This implies that the existence of a right may not necessarily be a *sine quo non* for granting of inventorship.[170]

To demonstrate consistent reference to a natural person as an inventor, EPO referred to the legislative history as contained in the *Travaux Préparatoires* for the Convention. According to these records, the possibility of recognizing the inventor as a legal person arose but was not included in the final draft.[171] In the final analysis, EPO held that presently AI systems have no legal personality comparable to legal or natural persons and as such are not capable of exercising rights.[172]

3.11 Emergence of new fundamental rights

Despite the fact that the Universal Declaration of Human rights is not legally binding, it serves as a source upon which human and fundamental rights are derived and evolved over time. It therefore remains as a source for all these rights, and it has informed subsequent binding and non – binding international, regional and national instruments regulating human and fundamental rights. Key to these instruments include the International Covenant on Civil and Political Rights[173], the European Convention of

---

[170] Thaldar, D. and Naidoo, M. (2021) "AI inventorship: The right decision?", *South African Journal of Science*, < AI inventorship: The right decision? | South African Journal of Science (sajs.co.za). (05 August 2022).

[171] *Travaux Préparatoires* is a French concept meaning official records of negotiations. There have been references in various documents such as a person, jointly made by several persons, employed, or a person designated as the inventor.

[172] For example, the legislative framework in various member states to the EU specifically make reference to natural or legal persons as the only one capable of being an inventor. As a result, section 1(1) of Danish Consolidate Patents Act, section 1 Finnish Patents Act 550/1967 as well as Ss 6, s37b German Patent Act, Articles 8, 11, 20, 22, 32 Polish Industrial Property Law, Article 1 Swedish Patent Act as well as Section 13 UK Patents Act. This can be seen from the Danish Consolidate Act No. 90 of 29 January 2019 The Consolidate Patents Act (Consolidate Act No. 90 of January 29, 2019) (wipo.int). < (11 December 2022).

Human Rights and African Charter amongst others. In South Africa, these rights are contained in Chapter 2 of the Constitution of South Africa and related secondary legislation.[174]

New technological developments in the form of Internet of Thins, AI, Blockchain technology and sophisticated algorithms are bound to have a significant impact on existing human and fundamental rights on the one hand, and on the other hand have a potential to give rise to new rights. Based on discussions above, it is clear that most of these potential rights would not be able to be accommodated by existing legislative and regulatory frameworks.

The impact of these technologies can be seen in three ways.[175] Firstly, the violation of rights, conflicting rights and new issues all emanating from usage of new technologies. The violation of rights may arise when AI analytics systems interferes with privacy rights or when risk - profiling tends to discriminate against any individual. Conflicting rights may arise in instances of using AIS for intelligence gathering in the interest of public safety and corresponding right to privacy. New issues would include the right to anonymity, to oblivion or not to be forgotten as provided for in Article 17 of the EU GDPR.

Contemporary regulatory landscape for AIS attempts to address their undesirable impact while also striving to enhance innovation and

---

[173] The International Covenant on Civil and Political Right was adopted on 16 December 1966 and initially signed by 116 state parties, currently it has been ratified by 173 of the 193 UN Member States, with South Africa and significant number of EU Member States embracing the Covenant.

[174] The European Convention of Human Rights came into force on 03 September 1953 and acceded all the 27 Member States

[175] The while the African Charter came into force on 21 October 1986 and acceded to by South Africa on 09 July 1996.

technology development. To a large extend, there is some degree of legal uncertainty of how existing legislative and regulatory frameworks addresses the violation of existing rights as well as conflicting rights. This leaves citizens exposed to potential violations with no or less legal protections.

These rights were drafted and embraced by many years ago,[176] and they were formulated in general terms aligned with ethical and societal values as opposed to specific situations and environment. While the rights were widely phrased to provide for sufficient space for interpretation and application, the values underpinning these rights have fundamentally evolved and changed.[177] This is attested to by Custers, who argue 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 does not only demonstrate regulatory gaps on privacy rights, but it also applies to many other fundamental and human rights threatened by usage and deployment of AIS.

In order to identify these gaps, Custers argues that assessment of how these rights apply in practice may result in stretching interpretation of existing legal framework and possibly yielding untenable distortions which may drift away from how the rights were originally conceived leading into legal uncertainty.[178]

To this end, the EU has adopted the Declaration on European Digital Rights and Principles for the Digital Decade in January 2023, as a

[176] For instance, the ECHR/GDPR were adopted and ratified in the 1950s when there was no computers, internet or algorithms.

[177] Bart Custers, New digital rights: Imagining additional fundamental rights for the digital era, Computer Law & Security Review, Volume 44,2022, < New digital rights: Imagining additional fundamental rights for the digital era - ScienceDirect (09 March 2023).

[178] Custers 5.

commitment to safe, secure and sustainable digital transformation prioritizing European people underpinned by European core values and principles.[179]
The principles are shaped around 6 themes:

- Putting people and their rights at the center 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
- Promoting the sustainability of the digital future

In assessing this Declaration and digital rights it proposes, a discussion of specific digital rights identified in literature across the board follows below.

3.11.1 The right to internet access or the right to be online

Internet access has become so critical in the 4IR as most of the services and products are only offered and available online, sometimes reasonably cheap and expensive if purchased offline. Inability and obstacles further put people in a disadvantageous position especially when it comes to public services job applications, access to social services and submission of online tax returns.

To ensure access to applications for social relief grants, the South African government used electronic systems in 2020 during Covid 19 state of disaster. Most of the applicants find it difficult to submit their applications

[179] European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)European Declaration on Digital Rights and Principles | Shaping Europe's digital future (europa.eu) (07 March 20230).

online due to lack of access to free internet. According to the collaborative study by National Income Dynamic Study, the applications systems collapsed and this delayed payment of such grants.[180]

It must also be indicated that Article 19 of the Universal Declaration of Human Rights takes recognition of the right to internet, which give effect to the right to freedom of opinion and expression as well as access to information.[181] In particular, to give effect to the right to internet, the UN Human Rights Council passed a resolution declaring access to internet as a catalyst to the enjoyment social, economic and cultural rights in 2021. However, the UN stopped short of boldly recognizing this particular right and as such it does not have a binding force. The resolution was adopted in anticipation to accommodate future technological developments.

The African Commission on Human and People's Rights adopted a Declaration of Principles on Freedom of Expression and Access to Information in Africa in 2002, which was later updated it in 2019. The Declaration is geared at accommodating some of the novel but shadowed digital rights occasioned by the 4IR.[182] It states that the "universal, 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 could however be observed that conditions on the ground show that this principle is still far from being

[180] Wills, G, van der Berg, S, and Mpeta, B. 2023. Household Resource Flows and Food Poverty During South Africa's Lockdown, Short-term Policy Implications for Three Channels of Social Protection. < https://www.uj.ac.za/wp-content/uploads/2021/10/nids_cram-wave-1.pdf (08 March 2023).

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

[182] Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2002 < Declaration of Principles on Freedom of Expression 2019 | African Commission on Human and Peoples' Rights (au.int). (22 December 2022).

realised. The precondition for access to the internet is access to a stable power supply. According to the World Bank, only 46.5% 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 is 39.3% of the population in 2020, compared to 62.9% in the rest of the world. Within the continent, regional and national differences are extreme, with 59.5% of people in Southern Africa having access to internet.[183]

*3.11.*2 The right to be offline or to disconnect

This right is currently applicable within the context of employment law, whereby in some countries employees are entitled to a right to be offline or to disconnect especially after working hours. The right presupposes that employees may not be contacted by the employers or their representatives outside working hours and days through any form of communication. These include through 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 having some social benefits especially in dealing with issues of internet addiction and its negative impacts in society. From a social point of view, it is clear that compulsive and excessive use of internet that is uncontrollable, especially social media to tends to cause considerable anxiety problems that affect mental health and well – being of individuals. Therefore, the right to be offline and disconnect is expected

---

[183] Hendrik Bussiek, Digital Rights are Human Rights, An introduction to the state of affairs and challenges in Africa, April 2022. < https://library.fes.de/pdf-files/bueros/africa-media/19082-20220414.pdf (09 March 2023).

to set and enhance necessary standards and expectations to prevent addictions and help people to become productive members of society.

3.11.3 The right to change your mind

Most websites would seldom require a person to enter their personal details and their preferences of what they want to see or know about. In this way, one is required to disclose their individualised preference which are then capture by algorithms to determine the kind of information, products and services can be offered to you by inference.[184] For instance, if you are interested in arts and politics, anything to do with these topics would be fed to you.[185]
As a result, people end up in what is known as filter bubbles, resulting in them being stuck and bombarded with feedback loops of information. Every time you log into your computer these kind of information graces your screen. In psychological terms, this result in a phenomenon known as cognitive dissonance because the information is fed back in contents and formats in accordance with their perceptions and convictions.[186]

The critical question is what happens when a person changes their mind and no longer interested in arts and politics. Attempts to change the settings may not be helpful in that algorithms may try to prevent this, leaving to be stuck in filter of bubbles and echo chambers due to previous preferences and interest.

While Article 18 & 19 of the UN Universal Declaration of Human Rights read together with Article 9 and 10 of the ECHR guarantees the

---

[184] Pariser, E. The Filter Bubble: What the Internet Is Hiding from You. New York, (May 2011), Penguin Press 17.
[185] Festinger, L. (1962) Cognitive dissonance, Scientific American. 207 (4): 93-107.
[186] Pariser, E. (May 2011) The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press 17.

fundamental right to the freedom of thought and expression, current technological developments demand a renewed and stronger protections to these rights. These protections would go a long way in reinforcing the right to change your mind by putting more weight on values around informed consent, online freedom and personal development amongst others.

3.11.4 The right to know the value of your personal data

While the provision of most online services and products such as search engines and social media platforms are freely available with no financial costs, companies offering these services makes profit by collecting, leasing and trading personal data on their systems. Therefore, people are being duped into believing that accessing these platforms is free despite the fact that there is no free lunch in this world.[187]

From a financial and economic perspectives, it would seem like there is no transparency on how these data is processed. It is entire unclear how the value of personal data is weighed and valued, including its worth. Therefore, it is only valid that consumers using these platforms are entitled to exercise their right to know the value of their data.

The application of privacy rights would not be feasible and adequate to protect commodification of personal data collected from search engines and social media platforms. For these reasons, it would be important that determination of any value attached to personal data as a commodity to

[187] Malgieri, Gianclaudio and Custers, Bart, Pricing Privacy – The Right to Know the Value of Your Personal Data (2017). Malgieri, G., and Custers, B. (2017) Pricing privacy: the right to know the value of your personal data, Computer Law & Security Review. < https://ssrn.com/abstract=3047257.(10 March 2023).

include pricing models, bodies responsible for determining pricing and how this should be enforced.

3.11.5 The right to 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 private sector to strive for clean environment.

The continued efforts to digitize the world and narrow the digital divide comes with 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-wastes across the supply chains within the digital corporate world. An example would be the use of blockchain technologies, which tends to use or generate a very large amounts of energy which may put pressure on the environment.[188]

According to Coalition for Digital Environmental Sustainability (CODES), the digitalization process would be crucial in achieving the UN's Sustainable Development Goals (SDGs) by 2030. To this end, an assessment by CODES in 2020 found that 70% of 169 targets base-lining the world's sustainability goals can be positively influenced using digital technology applications.[189] Therefore, this implies that technologies dominated by AIS will pay an influential role in environmental sustainability.

---

[188] De Vries, A. (2018) Bitcoin's Growing Energy Problem, Joule, Volume 2, Issue 5, p. 801-805; Dittmar, L., Praktiknjo, A. (2019) Could Bitcoin emissions push global warming above 2 °c Nature Climate Change, 656-657.

[189] Polina Koroleva, Action Plan for a Sustainable Planet in the Digital Age.31 May 2022 < CODES_ActionPlan.pdf (unep.org) (10 March 2023.

With digital traces everywhere, it could therefore be argued that data would be the pollution issue in the 4IR. Combined with other data, digital pollution may result in digital biases and noises when sucked in the aggregation of data analysis thus resulting in the pollution of the online ecosystem.

3.12 Role of soft law in the development and governance of AI systems

To begin with, soft law can be defined as international norms, rules, and principles that guide state parties 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. Although it may have certain legal effects, it is not binding, nevertheless. It serves to close the unregulated gap while guiding states and other stakeholders in the absence of binding legal norms. In the absence of a clear legislative instrument regulating the recognition and governance of AI systems at the international level, a credible body of soft law rules has been established at least formally at regional and national levels.

The abrupt surge of the coronavirus pandemic in early 2020 spurred many jurisdictions into action to legislate and regulate various aspects of societal life to contain and control the disease. Some of these legislative measures were seen to be draconian as they tempered some of the fundamental rights. Various organs of the United Nations also joined the bandwagon by issuing regulations and policy guidelines as part of disease management.[190] However, the international community could not apply the

[190] The United Nations through the World Health Organisation went to great lengths to ensure that the diseases are mitigated and controlled. Some of the guidelines and policy directives are found here <https://www.ohchr.org/en/covid-19/covid-19-guidance. (29 June 2022).

same energy and zeal in tackling the emergence of artificial intelligence in the 4IR.

Perhaps self-regulation of AI systems by corporate companies should be left to unfold because it may work to the advantage of humanity, as some scholars have argued. The disadvantage of this is that if left self–regulated humanity might lose the only opportunity available to assert itself over it before it could surpass human beings. On the other hand, subjecting AI to hard law is seen by others in a negative light because this may be tantamount to scuppering 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 in an attempt to regulate AI, at least at the operational level. This partnership has gone to great lengths such that an implied consensus has been established on the basics of the management and governance of AI systems. Various agreements and conventions have been adopted and complied with. Most of these agreements are based on and guided by important international instruments such as the UN Charter on Human Rights.

To establish some regulatory framework, various state parties and stakeholders have committed themselves to using the advantages of AI and minimizing possible risks inherent in its use. To this end, state parties and regional bodies have adopted some agreements and treatises, together with the private sector.

In the EU, the Ethics Guidelines for Trustworthy Artificial Intelligence and an Assessment List for Trustworthy AI have been agreed to by state parties. The Guidelines identified key principles and requirements for Trustworthy AI and the Assessment List which provides a framework in support of ensuring compliance with ethical standards by developers and

users of AI. The guidelines also address issues of data protection, algorithmic transparency, and openness amongst others.

A central piece of EU secondary law in the context of AI is the General Data Protection Regulation, which regulates automated processing of personal data in the European Economic Area. This is key in safeguarding fundamental rights in the context of the use of AI and related technologies. The Treaty on the Functioning of European Union adds am impetus by laying down principles of non – discrimination as one of fundamental values especially in Articles 2 and 10, which requires the Union combat discrimination in listed grounds.

The European Union Charter on Human Rights serve as a primary regional instrument indirectly and directly providing a basis for regulation of AI systems. This can be seen in Articles 20 and 21 which provide for equality before the law and non-discrimination. This is further elucidated in a raft of non-discrimination directives, with varying scope of application, which enshrines more detailed sector-specific legislation and directives aimed at safeguarding fundamental human rights.[191]

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 been put in place already. The proposals for the AI treaty contain key values which are mostly derived from the OECD's five Principles on AI.[192] The principles include the following:[193]

---

[191] They include the Employment Equality Directive (2000/78/EC), Racial Equality Directive (2000/43/EC), Gender Goods and Services Directive (2004/113/ EC), as well as the recast Gender Equality Directive (2006/54/EC). In addition, majority of the EU Member States are also party to other international human rights conventions.

[192] In May 2019, the OECD AI Principles were adopted by 40 countries in the west for innovation and trustworthiness in terms of human rights and democratic values by setting standards that are practical and flexible enough to stand the test time. <The OECD Artificial Intelligence (AI) Principles - OECD.AI. (03 July 2022).

[193] OECD's five Principles on AI.< https://oecd.ai/en/ai-principles/. (03 July 2022).

> that 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. Organizations and individuals developing, deploying, or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Currently, there is sufficient rules of soft law that have been developed and entrenched to cope with the deployment and usage of AI systems globally. While the rules are not binding, some possess some degree of enforceability and are compulsory to comply with.

3.13 Conclusion

The usage and deployment of AI systems are bound to dominate every aspect of life as the world tithers on the cusp of the 4IR. The international community is faced with two choices, to legislate or let self–regulation take its course. Equally, both routes have their advantages and disadvantages. Given its propensity to harm while bringing in incentives for the benefit of humanity, a careful approach to legislating it seems to be the option the international community needs to consider.

In today's world, a mere click on a technological device may sound more like signing away all your entitlements. If not managed well, data collection methods and mechanisms require an urgent careful approach. Most of the

global data for AI takes place in the developed world given their proximity and access to technological aid. Because algorithmic data for AI is sentient and susceptible to subliminal biases, it becomes imperative that the international community intervene urgently and regulate. Failure to act accordingly, may as well result in reversing significant progress made especially in terms of human rights as well as development of humanity.

The international human rights regime plays a pivotal role in balancing the power between an individuals and state. These rights serve as a foundational value for a democratic and open society. The protection and defence of fundamental human rights is also a springboard for the enjoyment of the sanctity of humankind and its concomitant development and well-being, both online and offline dominated by a growing algorithmic and data-driven society.

An apparent lack of transparency and accountability by regulatory regimes on intellectual property does not augur well in a world facing a transition to an era dominated by technology and artificially intelligent. It is hoped that the developing world would not face the same situation as when the vaccine for coronavirus was developed and distributed. The development, production, and distribution of AI technologies must be underpinned by principles of accessibility, explainability, openness, and transparency if multi-national corporates are to be held accountable.[194]

[194] Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI: Opening the Black Box or Pandora's Box Communications.

Chapter 4: Regulation of AI Systems in the European Union

4.1 Introduction

AI systems are bound to dominate the 4IR era in an unprecedented manner. Therefore, the discussion will explore the impact and positioning of AI systems as one of the key defining features of the 4IR. Of particular importance, is whether and how rights, duties, and obligations deprived or enjoyed by AI systems affect the legal systems. The extent to which the legal system accommodates and handles AI-related issues will also be put under the spotlight.

The discussion in this chapter proceeds by reflecting on the background regulation of AIS in the UE and concludes by recognizing the much progress has been made in dealing with various legal aspect of artificial intelligence systems. This can be seen on the risk – based approach adopted by the EU in regulating these systems. However, lack of consensus on the definition and legal personality of AIS proves to be a drawback when it comes to liability and accountability issues.

It is also interesting to establish that the EU legislative proposals have made strides in refining and adapting various liability rules aimed at holding accountable various corporate stakeholders, within the context of the value chain. The chapter concludes by noting and progress and lessons that can be drawn by interested jurisdictions wanting to regulate AIS.

4.2 Background on the regulation of AI systems in the EU

The European Commission (the Commission) is an executive branch of the European Union (the Union) consisting of representatives from 27 member states, nominated by the European Council and endorsed by the European Parliament while others are seconded by their national parliaments and governments for a 5-year term of office.[195] The Commission administers daily activities of the Union such as policy development and implementation, budget administration as well as monitoring and compliance. Members of the Commission are appointed to

[195] The UK has withdrawn from the EU in 2020 through a timeline set out in Brexit, while Iceland, Norway, and Liechtenstein are not part of it though they fall within the European Economic Community.

advance the interests of the EU and not necessarily those of their countries of origin.

In conducting its policy and law-making responsibilities, the Commission consults with member states, parliaments, and a broad spectrum of stakeholders amongst others. Legislative proposals of the Commission are further subjected to scrutiny by the European Parliament and European Council, which has a final decision on all laws to adopt, amend or reject.

Against this backdrop, the Commission released a raft of legislative proposals in 2021, aimed at harmonizing and approximating the regulation of AI systems EU Regulations[196]

These legislative proposals are based on Article 144 of the TFEU which seeks to harmonize and approximate EU laws to reduce trade barriers and improve the internal market.[197] The consumer protection laws and directives passed over a decade ago in 2008 laid a solid basis in regulating AI systems in the EU. This came in the form of Unfair Trading Regulation 2008 which sought to implement EU Directive 2005/29/EC aimed at harmonizing consumer protection laws in EU member states and curbing unfair commercial practices.[198] In addition, the regulations were also aimed at assuring consumer confidence and product safety for consumers to transact across EU state borders with ease.[199]

The horizontal nature of the draft legislative proposal would require to be consistent with existing Union legislation, especially those that are sector – specific such as the high risk categories and are currently being used or likely to be used.[200]

---

[196] The Proposal for Regulation in the European Parliament and Council in Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. (09 October 2022).

[197] It should be noted that the Treaty on the European Union and the Treaty on the Functioning of the European Union was adopted in Lisbon by 27 member states in 2007 and entered into force in 2009 to constitute the basis of European law. < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A12008E114 (09 October 2022).

[198] The 2005 EU Directive is to ensure there is proper functioning of the internal market and also to achieve acceptable levels of consumer protection by harmonizing and approximating the laws, regulations, and administrative provisions of the Member States on unfair commercial practices. < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02005L0029-20220528&from=EN. (09 October 2022).

[199] Osborne Clarke Unfair commercial practices law summary, 03 Jul 2008.< Unfair commercial practices law summary | marketing law (osborneclarke.com). (09 October 2022).

[200] EU Proposal 4.

Most importantly, it is also imperative that there is consistency with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection. Without compromise, the proposals have to comply with the requirements of the GDPR. The same applies to consumer protection and non-discrimination, including the imperatives of gender equality.[201]

Furthermore, the proposal complements existing Union law on non-discrimination. At the core of this, the minimization of algorithmic discrimination starts the collection, design and quality of data sets that are used for the development of AI systems. As part of quality assurance and standardization, the Proposals makes it an obligation to subject AIS to testing, risk management and documentation as well as human oversight before releasing them to the market and throughout their lifecycle. Most notably, the proposals also applies to competition law as they integrated into the existing sectoral safety legislation to ensure consistency, avoid duplications and minimize additional burdens.

Flowing from above, one could argue that, as a harmonized and unified block, that the EU would be well positioned to mount an influential lobby to ensure its position on AIS is endorsed by the international community. However, the US, Russia and China are also making notable advances in this area which could similarly influence international approach. Unfortunately, the latter jurisdictions do not form part of this work.

4.3 Definitional challenges of AI systems

While the primary question that the current legislative proposals seek to answer is legislation and regulation of AI systems, they fell short in defining the subject itself. In the initial stages, the proposals attempted to assign a definition, but the EU Parliament strategically declined to do so owing to industry pressure in the main. No universal definition has so far been established, as indicated earlier on.

Since the concept of "artificial intelligence" came into the picture over the last 70 years, there has not been a universally accepted definition up to this point. [202] John McCarthy, who famously coined the term in the 1950s,

[201] In this regard the EU Directive (EU) 2016/680), provides for approximation and harmonization of the rules in relation to designs, development, and use of certain high-risk AI systems and further places restrictions on certain uses of remote biometric identification systems.

remarked that because there is no “solid definition of intelligence that doesn't depend on relating it to human intelligence we cannot yet characterize in general what kinds of computational procedures we want to call intelligent”. This demonstrated difficulty associated with characterizing the AIS, and ultimately its legal status.

The extensive discussion on possibilities of conferring AIS with a legal personality status was rescucitated after the adoption of the 2017 Resolution on Civil Law provisions on Robotics by the European Parliament.[203] In terms of this resolution, the Parliament intended to create a specific legal status for robots that could in the long run accommodate even the most sophisticated autonomous robots. In this way, it aimed to confer AIS with some legal status which would ensure that it can be held responsible for making good any damage it may cause independently to third parties. Informed by this understanding, one of the European legislators then proposed the concept of “electronic person” as applicable to robotics. However, this position was abandoned in subsequent legislative proposals as indicated elsewhere in the study.

According to the European Parliament, any definition purporting to be describing cyber-physical systems and intelligent autonomous systems should be based on the following standards and characteristics of intelligent robots:

> ‘gaining autonomy through sensors or exchanging data with the environment (interconnection) and exchanging and analysing these data; self-education capacity based on experience gained and interactions with the environment (optional criterion) and at least minimal physical form; adaptation of behaviour and actions toward the environment; and lack of life functions in a biological sense’.[204]

---

[202] Martin Ebers, Liability for Artificial Intelligence and EU Consumer Law, (2021), Journal of Intellectual, Property, Information Technology & Electronic Communication, L 204. <https://heinonline.org/HOL/P?h=hein.journals/jipitec12&i=211. (08 October 2022).

[203] Paweł Nowik, Electronic personhood for artificial intelligence in the workplace, Computer Law & Security Review, Volume 42,2021, https://www.sciencedirect.com/science/article/abs/pii/S0267364921000571?via%3Dihub. (08 October 2022).

[204] The European Parliament resolution and recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), 16 February 2017.< https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051 (10 October 2022)

The 2017 Recommendations to the European Commission calling for the creation of a new category of legal personality for the most advanced AIS, was mainly motivated by the fact that this could solve the issue of civil liability for damages in the most dubious cases. According to the current Proposals, there are two options capable of addressing liability constraints arising out of damage caused by AI. Firstly, a strict liability (no-fault), and secondly a risk management approach (liability of a person who has been able to minimize the risk). These rules are underpinned by the basic principle that liability or responsibility should be proportionate to the actual level of instructions given to the robot and the degree of autonomy of the robot.

4.4 Adopting different rules for different AI systems

To ensure that the regulatory intervention is proportionate, the EU draft legislative proposals on AI identifies five categories in terms of potential risks they pose.[205] Accordingly, this approach presupposes that policymakers and regulators should apply stricter rules to preventing potential harms and losses prevalent in high-risk AIS on the one hand, and on the other provides for more permissive rules for low-risk AIS to reduce compliance burdens while promoting experimentation exercises.

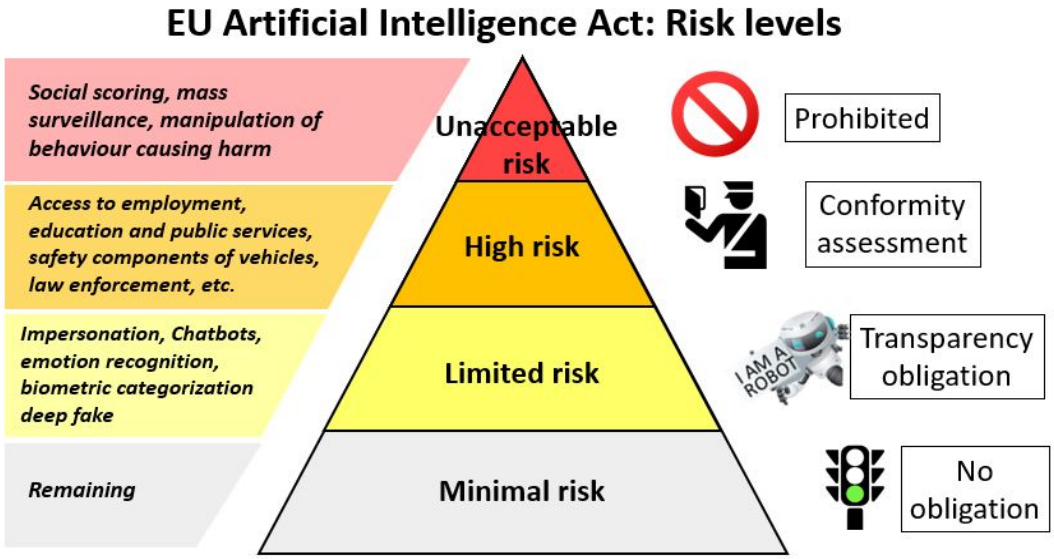

Figure 1: Risks levels in terms of the EU Artificial Intelligence Act: (*Source: Telefónica*)[206]

[205] EU Proposals Annexure III.

A risk-based approach to AIS is provided for in Annexure III of the proposals and identifies four risk categories of AI systems.[207] Article 67 requires that AI systems falling in both unacceptable and high-risk categories are required to be marked for clear identification.[208] According to the EU AI Act, the regulatory obligations are measured by the risk each AI system poses and they are differentiated in terms of unacceptable risk, high risk, limited risk, or low or minimal risk.[209] This risk-based approach is regulated according to different standards, and they can be delineated as follows:

4.4.1 Unacceptable risky AI systems: Risk category #1

The proposed legislative proposal in the EU prohibits practices that unacceptably risky are categorised as Risk category #1. These are the kind of risks that are even banned in some jurisdictions. They categorised in this manner because they have a high potential to violate fundamental human rights, subliminally manipulate people and exploit vulnerable groups such as children and the women. The systems in this category also have the propensity cause psychological or physical harm as well as perform social scoring for use by private and public authorities.

The introduction of the AI Act imposes a moratorium on facial recognition systems, except for specific law enforcement purposes if accompanied by an independent authorization regime. While the collection of real-time remote biometric data in public spaces for law enforcement purposes may be justified, this must be carried out cautiously to avoid infringement of human rights.

According to studies by UK's Information Commissioner's Office, there are indications that biometric recognition systems are currently being used in about 11 EU member states, while about 8 are to follow suit. However, this is not carried out in real-time but as part of *ex–post facto* identification exercise, where video footages are scrutinized after the incident.[210]

---

[206] Figure 1 < https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/09/Pir25C325A1mide2Bingl25C325A9s.jpg. (11 October 2022).
[207] EU Proposals Annexure III.
[208] In terms of EU Proposal Article 67, to show that high-risk AI systems comply with EU regulations, they must bear a CE marking as this would enable them to move freely within the internal market.
[209] Figure 1.

According to the study, the distinction between real-time and *ex-post facto* identification is viewed as irrelevant especially when it comes to the impact of these technologies on fundamental rights. As a result, ex-post identification carries a higher potential of harm, as more data can be pooled from different sources to proceed to the identification.[211]

Because of their controversial nature, it is not clear whether the prohibitions in this category will make a final cut when the Act is finally passed into law and binding. Sustained pressure from the industry may result in the removal of some of these practices in the recommendations by the High-Level Expert Group on AI.

4.4.2 High-Risk AI Systems: Risk Category #2

The AI systems that constitute Risk Category #2 relates to softwares that have the potential of creating risks to human safety, health, or fundamental rights. This criterion contemplates sectors with potentially significant legal risks, especially in areas of transport, energy, transport, and parts of the public sector. The legal effects may result in damages, injury, and death due to the application and deployment of AI systems in a particular sector.[212] Because the category is deemed high risk, the AI Act sets out pertinent requirements relating to human oversight, the accuracy of the information, and robustness which must be provided by producers.

These kinds of systems may operate subject to certain conditions, having undergone ex–ante conformity assessments before putting them on the market. In addition, the systems ensure quality assurance in terms of data quality, and traceability when documentation is submitted to regulatory authorities.[213]

---

[210] It is reported that law enforcement agencies in EU countries such as Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Slovenia, and the Netherlands have deployed facial recognition technologies for *ex-post* identification in recent years. It is also reported that plans are afoot to implement these systems countries like Croatia, Cyprus, Czechia, Estonia, Portugal, Romania, Spain, and Sweden. Facial recognition technologies already used in 11 EU countries and counting, report says, Luca Bertuzzi | EURACTIV, October 28, 2021. Facial recognition technologies already used in 11 EU countries and counting, report says – EURACTIV.com (12 October 2022).

[211] Guide to Data Protection | ICO (12 October 2022).

[212] Thomas Hoerber, Gabriel Weber and Ignazio Cabras. Artificial intelligence in the European Union Policy, ethics and regulation, 2022, The Routledge Handbook of European Integrations, Inga Ulnicane

[213] Artificial Intelligence Act, Securiti https://securiti.ai/eu-artificial-intelligence-act/ (11 October 2022).

This category of high-risk AI systems must comply with transparency and explainability requirements. It is obligatory to inform and advise end–users that they are interacting with AI systems and not human beings. Amongst others, the European Commission lists critical infrastructures that could endanger citizens' lives or health, credit scoring, border controls, transportation, and employee management systems.

In applying requirements of transparency in the workplace, the Court of Cassation (Supreme Court) in France has held that “the employee has the right, even at the time and place of work, to respect for her privacy, which implies, in particular, the confidentiality of communication."[214]. The reasoning of the court was in line with the provisions of Article L 1121 – 1 of the French Labour Code which stipulates that no one shall limit individual or collective rights unless it is justified in relation to the task to be performed or proportional to the goal they are aimed at. This underlines the obligation placed on employers to inform sufficiently whenever surveillance systems are used to monitor employees and the potential to intrude in their personal life. This further demonstrates the extent of harmonization laws brought about by the EU proposals.

4.4.3 Limited Risk AI Systems: Risk Category #3

This category requires compliance with stringent disclosure requirements by producers of AI systems.[215] Providers of these systems are required to ensure that natural persons are notified about their engagement with AI systems unless the context and circumstance dictate otherwise. This is to ensure that natural persons have the freedom to exercise their right of choice.

Under the category, transparency requirements require users of recognition technologies and emotic biometric systems to offer explanations to affected persons of how these system operates, including implications thereof. This also include the usage of controversial

---

[214] Cour de Cassation, Chambre Sociale [Labour Division of the supreme court] October 2, 2001, No. 99-42.942 (Fr.). < https://www.legifrance.gouv.fr/juri/id/JURITEXT000007046161/. (11 October 2022.

[215] Art. 3 of the Product Liability Directive defines a producer as the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer. Without prejudice to the liability of the producer, any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business shall be deemed to be a producer within the meaning of this Directive and shall be responsible as a producer.

technologies such as deep fake technology or systems which create or manipulate photos, videos, and audio content.[216] The AI Act imposes disclosure obligations favourable to users of this technology. The disclosures in questions may include whether the content of the technology used has been artificially generated or manipulated. This is aimed at ensuring that the public or people with interest are not deceived by these technologies.

However, these transparency obligations does not apply to AI systems that are authorized for law enforcement purposes unless such systems have been made available to the public for purposes of reporting criminal activities.

4.4.4 Minimal Risk AI Systems: Risk Category #4

Amongst others, the AIS systems included in this category relates to technologies that are used for spam filters and video games. These technologies poses little to no harm insofar as personal safety and human rights are concerned. Most AI systems currently in use fit squarely into this category. The Proposed legislative provisions do permit unrestricted use of these applications without imposing any new requirements.

Critical to risk–based approach is the question of whether it should be dealt with in terms of a precautionary or permissive way. In the first place, a precautionary approach is intended to achieve what is known as ex-ante protections to mitigate potential harms that may occur beforehand.[217] This could be the case where state entities, relying on hard or soft law instruments set out guidelines and requirements to comply with certain standards before AI systems are deployed.[218]

---

[216] Riana Pferpferkorn, Deepfakes in the Courtroom, Public Interest Law Journal, Vol 29, 2020, Center for Internet and Society, Stanford Law School. < https://siliconflatirons.org/wp-content/uploads/2021/02/Pfefferkorn.pdf. (12 December 2022).

[217] Jose Felix Pinto-Bazurco, The Precautionary Principle, October 2020, Earth Negotiations Bulletin. < still-one-earth-precautionary-principle.pdf (iisd.org) (23 October 2022).

[218] This is attested by a UNESCO Report on 'Ethical Perspectives on Science, Technology and Society, 2015. < Ethical perspective on science, technology and society: a contribution to the post-2015 agenda, report of COMEST - UNESCO Digital Library. (10 October 2022).

In the second place, permissive approaches provide innovators of AI systems with more leeway to experiment and deploy AI systems without explicit government approval. However, the risk here is that they can be exposed to huge litigation costs and possible large fines as the proposed provisions are geared at discouraging reckless risk-taking. As a result of risks that could be apportioned to stifling of innovation through regulatory barriers, more weight is attached to a permissive approach as opposed to a one that adopts a precautionary approach. However, It would seem like a permissive approach, if well-designed, may still mitigate and prevent many undesirable outcomes as it has a room for greater experimentation and innovation.

The EU often employs the precautionary principle when designing certain regulations and legislation, and this has also been provided for in the AI Act. The precautionary principle is most notably used in EU environmental law as part of efforts to protect people from scientifically proven environmental hazards such as aerosol sprays which have the potential to deplete the ozone layer or unsustainable use of fishery resources. [219] Conversely, the United States has however embraced the notion of permissionless innovation as opposed to a precautionary approach which elevates AI systems in high regard thus limiting the enjoyment of their benefits by society.

Given the potential for AI to seriously disrupt society negatively, some experts are recommending a precautionary approach over a permissive approach so as to discourage excessive risk-taking by developers and engineers when building AI systems. Based on this, some experts also believe that many AI risks and uncertainties justify similar precautionary regulations in the digital environment. On general terms, most experts agree that a risk-based approach is necessary for regulating AI, though there is lack of consensus over the details and implementation thereof.

Considering available evidence, there is more support for a risk-based approach in regulating AI. The critical issue would only relate to how these risks are categorized and what should be in each category. It is also how the lines are drawn and how greatly this would affect accountability requirements which determines each risk category. Similarly, it is also important to take into account regulatory burdens for different AI systems.

---

[219] World Commission on the Ethics of Scientific Knowledge and Technology, UNESCO, *The Precautionary Principle*, 2005.<Results - UNESCO Digital Library (12 October 2022).

4.5 A human rights approach 'in the interests of the EU'

4.5.1 Product liability regime in the EU

As a point of departure, it is necessary to locate the right to a remedy that is effective as well as fair trial rights which are protected by Article 47 of the EU Charter of Fundamental Rights.[220], and its force is derived from Article 13 of the European Court of Human Rights. The Article states thus:

> that everyone whose rights and freedoms as outlined in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

It is therefore clear that the right provides extensive protections by guaranteeing effective remedies before the court of law. The Court of Justice adjudicated this right in a 1986 Johnston judgment, which asserted it as a general principle of Union law and applicable to all member states.[221]

According to Benhamou et. al, emerging digital technologies, including AI, are becoming increasingly complex due to the interdependency between:

> their different components such as *i)* the tangible parts/devices (sensors, actuators, hardware), *ii)* the different software components and applications, to *iii)* the data itself, *iv)* the data services (i.e., collection, processing, curating, analyzing), and *v)* the connectivity features.[222]

The digital economy of the 4IR remains to be dominated by a host of key merchants and corporates such as hardware manufacturers, software designers as well as sellers and equipment and software installers. In addition, there will also be facility owners, AI owners as well as AI users and trusted third parties amongst others.

---

[220] The Articles provides that everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended, and represented.

[221] Case no. 222/84, Johnston [1986] ECR 1651. Also important is Case no. C-97/91 Borelli [1992] ECR I-6313) on implementing Union law.

[222] Benhamou, Yaniv and Ferland, Justine, Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages (February 8, 2020). Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law, Forthcoming<: https://ssrn.com/abstract=3535387. (12 October 2022).

All of these would have a clear responsibility, along the value chain, to ensure that AI systems enjoys smooth sailing in minimizing and averting causation of harms and losses that would result in attracting legal liability and accountability. Given the existing liability regime, it would be an uphill task to properly identify and apportion liability to any of these players in the context of AI.

Because of the autonomous character of the AI system, the application of strict liability rules may prove to be impossible in determining which of the commercial parties, within the AIS value chain, is liable and accountable. Similarly, the current liability regime under product liability law seems to be inadequate to cater for harms emanating from the autonomous thinking of AI systems.[223]

Moreover, it may also prove futile to distinguish between damages arising from product defects from those resulting from AI's autonomous decisions. In most cases, this would put the plaintiff in a weaker position to demonstrate that the product was defective, even where proof of fault is required.

It was against the backdrop of this legal obsolescence that the EU Commission opted for two proposals to regulate product defect liability and AI liability regimes. The proposals relates to the recently released tools in the form of the Product Liability Directives and Artificial Intelligence Directives.[224] According to Bauwens, these proposals are mainly driven by the challenges the digital economy and AI impose on the directive's decade-old definitions and concepts. However, the new rules will apply more equally to all products, from garden chairs to medical devices.[225]

4.5.2 Liability for defective products

---

[223] Benhamou.

[224] The Proposals for a Directive of the European Parliament and of The Council on Liability for Defective Products. < COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products | Internal Market, Industry, Entrepreneurship and SMEs (europa.eu). See also the final Proposal for a Directive of The European Parliament And The Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive). < 1_1_197605_prop_dir_ai_en.pdf (europa.eu) (12 October 2022).

[225] Kathrin Bauwens - Mirjam Erb: < https://www.linklaters.com/en/insights/blogs/productliabilitylinks. Product Liability and AI (Part 3), Commission plans to overhaul EU product liability law, 29 September 2022. < https://www.linklaters.com/en/insights/blogs/productliabilitylinks/2022/september/commission-plans-to-overhaul-eu-product-liability-law. (12 October 2022).

Because of its omnipresence in every aspect of life, AI systems are set to raise novel complex legal questions in the area of product liability which are not accommodated in the current legislative framework. It has been an arduous task to pursue and enforce liability claims as a result of the characterization of AI systems. The difficulty is presented by the nature of AIS in terms of their opacity, complexity and their limited predictability as well as their semi-autonomous behaviour.

While the draft proposals for AI Act are aimed at ensuring that high-risk AI systems comply with safety and quality assurance standards, accompanying liability rules are geared at ensuring that it is possible to seek compensation when AI systems causes damages and losses.

In its Explanatory Memorandum, the Directive aims to ensure liability for manufacturers who bring defective products into the EU, including those outside its jurisdiction. This means that companies not operating physically present in the EU can be held liable if fails to comply with its laws if their services or products are accessible in the EU.[226]

The Directive are categorical in stipulating that not only hardware manufacturers would be liable, but also go as far as to bring into the fold software developers, providers, and providers of digital services for possible liability and accountability. It is therefore clear that anyone whose digital services determine how a product works can be held liable for defective products.

As a notable departure from the previous position and to strike some semblance of balance, is the advantage presented by the current EU Directives is in respect of the simplicity of locating the burden of proof. In addition, the restrictions associated with the lodgement of compensation claims have now been lessened. This would ensure that there is a fair balance between the legitimate interests of manufacturers, injured persons, and consumers in general. By confirming that AI systems, AI-enabled goods, and software are regarded as an in-scope products, the Directives affirms that compensation would be available when a damage is caused by a defective AI or software. In addition, this implies that an injured plaintiff doesn't have to prove the manufacturer's fault, and this

[226] The matter of cross-jurisdiction was dealt with in a German case to be discussed below, CJEU – Patrick Breyer v Bundesrepublik Deutschland – C-582/14 < CJEU - Patrick Breyer v Bundesrepublik Deutschland - C-582/14 - GDPR Beetle(12 October 2022).

alleviates the burden of proof in certain cases involving AI systems or/and when products fail to comply with safety requirements.

To top it, the proposals further makes provision for class actions to enable persons acting on behalf of others to lodge a strict liability action thus allowing mass consumer product liability claims in any of the member state, in line with a Directive on collective interests of consumers.[227] However, there is less to celebrate in this regard as the provisions for collective redress is limited and inconsistent across member states (such as Germany) while in others it has a broad scope. Similarly, qualified representatives are assigned to aggrieved consumers seeking redress, who may also be forced to be part of the action or opt-out depending on the nature of the action.

While the proposal hints to the exemption of manufacturers from liability under certain circumstances, they also proposes for adaptation of liability rules depending on the specific characteristics of digital and AI products in use at a particular point in time. The explanatory memorandum to the draft proposals suggest that it would be in the interest of consumer protection as this would level the playing field by exempting manufacturers for scientifically and technically undiscoverable defects. This is regarded as the state of the art defense. It is expected that these provisions would apply to all member states, though there is a possibility to derogate should they wish so.

While the ECJ expanded the definition of personal data in relation to IP address, it also reflected on the significance of cross-jurisdiction issues in adjudicating cases impacting on AI in the Breyer case.[228]The Internet Corporation for Assigned Names and Numbering (ICANN) is a US-based regulatory entity responsible for interconnectivity and compatibility for the effective operation of internet infrastructure and assigns Internet Service Providers (ISP) addresses globally through five regional registries. One of these registries is *Réseaux IP Européens* (RIPE), which is responsible for the distribution of ISP and general telecommunication providers to large corporates companies in Europe. It is through these channels that IP addresses are allocated to customers and clients.

---

[227] The EU Directive 2020/1828 on The European Parliament and of The Council on Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive 2009/22/EC, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020L1828&from=EN. (12 October 2022).
[228] Case C-582/14 Breyer v Bundesrepublik Deutschland ECLI:EU:C: 2016:779.

IP addresses are split into dynamic or static, the former being a temporary identification number while the latter is permanent enabling devices to connect to the internet. In addition, static IP addresses are suited for large business entities which require a fixed address in their servers for reliability and continuity. By reason of being fixed, it makes it easy to identify individuals and their geographical location through an IP address when a connected device is used, exposing the identity of the user contrary to EU privacy and data protection laws.

When a person, including Mr. Breyer, logs into the websites of the Federal German government their IP addresses are retained and stored as part of efforts to combat cybercrime. In contending with the matter, the German Federal Court of Justice sought an advisory note from the ECJ to interpret if IP addresses could be classified as personal data.

The ECJ handed down a landmark ruling in the Breyer case. The judgement declare that the dynamic IP addresses constitute personal data when the provider of a website has to access the additional information identifying data that is held by the relevant ISP. The basis of the decision was based on the expansive scope as provided for in Article 2(a) of the Data Protection Directives in the EU.

4.5.3 Liability for AI systems

As a centrepiece of the product liability regime in the EU, private individuals have at their disposal Product Liability Directive laws as a remedy applicable to claims against manufacturers on damages arising from defective products, damage to health, material losses due to loss of life as well as property or data loss. Conversely, AI Liability Directives have been proposed to serve as a second layer to a fault-based liability regime in addition to Product Liability Directives, the two operate hand in glove as instruments of liability.

The Directives apply to any person for fault-based claims on damages arising from malfunctioning AI systems. This includes damages by natural or legal persons claimable under national law such as those resulting from discrimination or violation of fundamental rights. Most importantly, the Directives explicitly eschew actions for criminal liability from its scope. To accommodate the fault-based liability regime, the basis of the proposals lie in the disclosure of information about AI systems involved. In addition,

there must be a presumption of a causal link between the AI system and the damage caused.[229]

4.5.4 Disclosure obligations

The object of the Directive affords claimants with a means to seek disclosure of information or evidence from potential defendants to enforce their rights for damages caused by suspected high-risk AI systems. As an avenue available to claimants, Article 3 (1) enjoins the courts to issue an order to this effect. The purpose of these orders also assists in correctly identifying potential defendants thus reducing caseload and litigation costs involved.[230]

Application for disclosure of evidence should be corroborated by facts establishing the plausibility of the claim contemplated and directed at the person who is subject to the provider's obligations in line with the provisions in Article 24 or 28 (1) contained in the AI Act. This is critical given a host of players in the AI value chain. Hence the requirements in Article 3(2) that such requests should only be directed at providers or users that are defendants unless all proportionate attempts were rendered unsuccessful.

The only limitation for disclosure of the information is provided for in Article 3 (3), which aims to protect and balance the proportionate interests of all parties considering business secrets and confidentiality obligations involved.

4.5.5 Presumption of causality

To relieve the claimant from the clutches of discharging the burden of proof, a presumption of causality has been availed in Article 4 of the Directive as a measure to address fair compensation. For a successful liability claim by claimant, it would be important that a causal link between the wrongdoer's act or omission is established. In relation to AI systems, this would mean that the act or omission giving rise to the breach of duty of care must have produced or failed to produce an output that resulted in the damage concerned.

---

[229] Breyer case para 7.
[230] Breyer case para 7.

However, according to the Commission it could be difficult to prove the causal link as this would require the claimant to explain the inner functioning of the AI systems, something which would require certain levels of expertise. As a result, the Proposals provides for a presumption that a causal link exists and further that if certain conditions are met.

A presumption of casualty would not be applied where the defendant is able to prove that a sufficient evidence and expertise are reasonably accessible for the claimant to prove the causal link. This would be the case where the damage in question involves high-risk AI systems. However, in claims where damages relate to AI systems that are not of high – risks, the presumption only applies if is highly difficult to prove a causal link by a claimant.

Regarding the long–term defects, the Report from the EU Expert Group on Liability and New Technologies has proposed the application of strict liability principles. This should be the case where the defects in emerging technologies emerge long after they were put into the market, provided the producer was still able to effect updates or upgrades to the technology in question.[231] Under the circumstances, the courts would not accept a development risk defence.[232] The rationale for this is that controls of the software through updates allow the manufacturer to remedy defects as they become known. However, defences of this nature could be prevalent in technologies involving cybersecurity standards.

The question of failure to update software development for AIS and accompanying fiduciary duty was considered by the UK Court of Appeal in Tulip Trading case.[233] In a decision that overturned the lower court ruling, the court, in this case, had to grapple with the question of whether developers of Bitcoin code owe a fiduciary duty to help the owner of a cryptocurrency to recover lost or inaccessible bitcoin after the owner's private key was hacked.

---

[231] Report from the Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technology' (European Commission 2019) [14].
[232] Matthew Channon, James Marson. The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles, Computer Law & Security Review, Volume 43, 2021.< https://doi.org/10.1016/j.clsr.2021.105628. (17 December 2022).
[233] Tulip Trading Limited v Bitcoin Association For BSV & Ors [2023] EWCA Civil 83, (03 February 2023 < Tulip Trading Limited (A Seychelles Company) v Bitcoin Association For BSV & Ors [2023] EWCA Civ 83 (03 February 2023) (bailii.org). (23 February 2023).

In this case, Tulip Trading Limited, the owner of $4 billion bitcoins which were held in two addresses on blockchain lost their private keys in a hack thus being unable to access or move them to safety. Before the court, Tulip contended that the defendants as the developers control and run the Bitcoin networks which would make it simple to secure and return control to its assets. It was also alleged that the bitcoins may not have been moved in the account because the hackers could not crack the encryption details which protected the private keys. However, Tulip maintained that it is not technically difficult for a patch to the computer code to transfer the digital assets to which access had been lost to a new address and regain the access.

In this way, Tulip raised a novel argument for the recognition of a new ad hoc class of fiduciary duties that is owed to the true owners of bitcoins. The duty in questions entails putting in place necessary software patches aimed at solving and safeguarding true owner from potential thieves within the virtual space.

This was challenged by the defendants who argued that access to the bitcoin addresses in question operates on a decentralized model and involves a large group of contributors in the software development who are attached to no organization or structure. They further asserted that any changes to the address would be ineffective as the earlier version of the software can only be effected by miners involved in the chain. To this end, the developers argued that it would be onerous and unworkable to maintain that they have control and owe fiduciary or any other duties to Tulip.

In deciding the matter, The Court noted the novelty of the issues in the case, especially in relation to categories of fiduciary relationships, and held that:

> the common law often works incrementally and by analogy with existing cases, and rightly so; but if the facts change in a way which is more than incremental, I do not believe the right response of the common law is simply to stop and say that incremental development cannot reach that far.[234]

The court highlighted that the features of novelty of the issues in the case were characterized by the presence of software and the code. The court

[234] Tulip Trading Limited case 86.

demonstrated by contrasting the usual physical coin which exists outside the minds of people and a bitcoin which exists outside the minds of individuals, but its properties exist outside computers due to software.

The court held that the overall control of a bitcoin source code for bank accounts lies with the software developers. The court held that this is unlike in the case of a bank, where software developers are entrusted with the responsibility of maintaining the source code of the bank's accounts and payment systems, subject to ultimate control by the board and existing regulations. In the case of banks, developers have no control over customers' assets while in bitcoins they have such control.

Amongst others, the court described the fiduciary duties of software developers to include making discretionary decisions and exercising power for and on behalf of other people who are entrusted with the duty of care in relation to their bitcoin properties. The content of the duties include a duty not to act in their own self-interest and also involves acting in positive ways in certain circumstances. In this case, such duty entailed introducing the code so that an owner's bitcoin can be transferred to safety in the circumstances alleged by Tulip.

To this end, Lord Justice Popplewell ruled that Tulip has raised arguable points of law which must be referred to trial where all the facts would be ventilated and adjudicated. The appeal was therefore upheld by the court.[235]

4.5.6 Proportionality principles

Once AIS causes harms or losses and it is uncertain from which party fault emanated, the principles of proportionality would kick in. In the first stage, proportionality principles would be limited to the burden of proof as well as measures aimed at identifying and addressing AI – specific problems. The process would include building on the substantive liability conditions as set out in the existing national rules. While this may relate to causality or fault, it would be more focused on targeted measures to ensure that victims are able to have the same level of protection as in cases not involving AI systems.

According to Taddeo, human beings are capable of exercising appropriate levels of judgment and remain responsible for the development,

[235] Tulip Trading Limited case 91.

deployment, use, and outcomes of AI systems.[236] While these principles accords with ethical frameworks applicable to AIS, it is not given that this would mostly be the case in the current age of technological development.

Therefore, it would be critical to source convincing evidence from the various tools available to ease the burden of proof. Otherwise, opting for rebuttable presumption it would be the least interventionist tool. It should however be noted that, such presumptions are commonly found in national liability systems, and they are largely able to balance the interests of claimants and defendants. At the same time, they are designed to incentivize compliance with existing duties of care set at the Union or national level.

It is there clear and a welcome move that the proposed legislative interventions in the EU would not lead to a reversal of the burden of proof, something which would have the effect of avoiding the exposure AI providers, operators, and other users in high risk AI systems. Such may also have the effect of hampering innovation and reducing the uptake of AI-enabled products and services.

4.6 Conclusion

The study has been able to establish that, as things stand, there are no concrete measures to regulate AIS in both the EU and South Africa. The regulatory efforts in both jurisdictions are more or less the same, as they are both fragmented though holistic. All that is required is to consolidate existing efforts, though the EU has made significant progress waiting for the current AI legislative process to unfold and conclude.

While the legislative proposals by the EU may be viewed as limited in terms of scope, they sure have far-reaching implications in various practical aspects. In this way, they have laid a solid foundation for future efforts to regulate and manage AIS in the long run. In actual fact, the proposals are in larger measures futuristic.

---

[236] Taddeo, M, McNeish, D. Blanchard, A. *et al.* Ethical Principles for Artificial Intelligence in National Defence. *Philos. Technol.* https://link.springer.com/content/pdf/10.1007/s13347-021-00482-3.pdf?pdf=button(17 December 2022).

The proposal in the EU further provides for an evaluation of various Directives and in the process envisages further instruments as additional measures necessary, especially in the areas of no–fault rules.

While the adoption of the Proposals would mark the beginning of a political process, it should be noted that compromises and agreements on envisaged amendments would be critical in finalizing the legislative process. Once adopted, harmonisation process will kick in with each member states expected to have some time to implement the Directives at their own pace but within stipulated timeframes.

And yet, companies which are involved in the development and management of AIS will have to ensure they are in a position to monitor the current legislative process. This would ensure that they are thoroughly prepared to implement appropriate risk prevention mechanisms in line with the requirements of enacted law. If adopted as presented, the accompanying Directives will generally set a new environment, particularly the proposed standards for a claimant-friendly litigation process for product liability in the case of harms and losses arising from AI systems. It would, however, be interesting how hurdles posed by the legal personhood of AI systems in the long run.

Most importantly, the draft AI Liability Directives have been subjected to public participation process and would operate for a period of five after which they will be reviewed. This is sufficient period to afford everyone an opportunity to participate in their implementation. After the completion of this period, the EU Commission shall thereafter make an assessment to ascertain whether the objectives were reached and, if necessary, propose further measures for adoption. By implication, this may include the introduction and consolidation of harmonized no-fault liability rules, including certain mandatory insurance for the operation of the AI systems.

The EU should be applauded for introducing initiatives especially those that are based on risk categories. The initiatives are simplified in a manner which could make them to be open for adaptation by any juridictions, South Africa included.

In South Africa, it remains to be seen if indeed processes would match up with progress made in the EU. This does not, however, mean that South Africa has no legislative framework regulating certain aspects of AIS.

Chapter 5: Legal accountability for Artificial Intelligence Systems in South Africa

5.1 Introduction

In South Africa, no tangible attempt has been made to embrace and regulate the legal conundrum of the use of AIS in the financial sector, particularly, the banking industry.[237] However, a raft of legislation and policy framework are in place to regulate transactions and activities in the financial sector without addressing the legal status of the systems.[238] South Africa will have to be innovative and creative in developing and adapting existing AI ethical principles on the deployment and management of AIS to remain relevant and competitive in a highly globalized economy.[239] Nevertheless, a solid basis is in place.

The digital economy of the 4IR remains to be dominated by a host of key merchants and corporates in the form of hardware manufacturers, software designers, sellers, equipment and software installers, facility owners, AI owners, AI users, and trusted third parties, amongst others.[240] All of these have a clear responsibility to ensure that AI systems enjoy smooth sailing in minimizing and averting causation of harm and consequently legal liability. Given the existing liability regime, it would be an uphill task to properly identify and apportion liability to any of these players in the context of AI.

---

[237] Stowe, A. A. (2022). Beyond Intellect and Reasoning: A scale for measuring the progression of artificial intelligence systems (AIS) to protect innocent parties in third-party contracts. Page Publishing Inc.

[238] See Ameer-Mia, Pienaar and Kekana "South Africa" in Berkowitz M (ed)(2020) AI, Machine Learning and Big Data 2nd ed, Global Legal Group Ltd London at 250.

[239] UNESCO Recommendation on the Ethics of AI, 2022 < Recommendation on the Ethics of Artificial Intelligence - UNESCO Digital Library. (19 September 2022).

[240] Benhamou, Yaniv and Ferland, Justine, Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages (February 8, 2020). Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3535387.(19 September 2022).

It should be reiterated from the onset that South Africa has no specific legislative instrument regulating AIS. However, the study in this chapter evaluate existing legislative enactments and policy framework which seems to lend credence to the feasibility of the recognition of AIS as legal persons. This discussion will also reflect on the impact and challenges companies must grabble with as the emergence of the 4IR intensifies.

Most companies in the financial and retail sectors are already deploying AIS in their variegated forms in their business operations.[241] Due to their strategic location in these sector, they use these systems in servicing both their customers and clients in the name of efficiency and effectiveness.

Equally, corporate management in the sector also uses AIS as support systems for decision – making at both management and board levels. Currently the systems are used as a guide to arrive at particular decisions that would enhance business productivity and profitability.

5.2 Assessment of AI development and regulation in SA

The State is positioned to play a central role in the planning and coordinating programs aimed at rolling out the implementation and management of AIS in the 4IR. To this end, South Africa is treating the novelty of 4IR technologies as opportunities for investments and funded experimentation through private-public collaborations. South Africa views its task as not only limited to deploying these technologies but also participating in their development.

The importance of this is emphasized by the HSRC, which argues that any policy alignment should be approached with the view of pursuing

[241] The study carried by Mckinsey Global Survey, indicates that there has been an increase of 12% from 45% to 57% of adoption of AIS by respondent companies in emerging countries in 2020. The State of AI2021, 18 December 2021. < https://www.mckinsey.com/capabilities/quantumblack/our-insights/global survey-the-state-of-ai-i n-2021.(16 March 2023).

developmental goals set by both the Sustainable Development Goals and the National Development Plan.[242] In order to deepen 4IR, it would be important to intensify necessary investments in areas of institutions of leadership in research, development, and commercialization in the area of AI as one 4IR technology.

To catapult South Africa into the 4IR, the Presidential Commission on the 4IR was established in 2019 and released its report in 2020.[243] Amongst the eight areas identified by the Commission, there are recommendations on the review, amendment and creation of policy and legislation on 4IR, including AI technologies.[244]

This is aimed at levelling the regulatory environment to ensure that it is adapted to enable the desired progress. In particular, the recommendation picks out the generation of intellectual property rights which stands out as part of the creative economy in the rapid production of new technologies, artifacts, and processes for commercialization and scale. Most interesting is that the recommendation goes further to place at the top of the agenda

---

[242] This is a conference held under the theme, Policy Options Framework for the Fourth Industrial Revolution in South Africa, An output of the Human Sciences Research Council, South Africa SA-EU Strategic Partnership Dialogue Conference Disruptive technologies and public policy in the age of the Fourth Industrial Revolution, 10 - 12 December 2018 CSIR International Convention Centre, Pretoria. < https://hsrc.ac.za/uploads/pageContent/10155/4IR%20Framework%20Report_Final_lowres.pdf (20 January 2023).

[243] Government Gazette No 42388, 19 November 2019, Terms of Reference for Appointment of Presidential Commission on the 4th Industrial Revolution. < https://www.gov.za/sites/default/files/gcis_document/201904/42388gen209.pdf.(20 January 2023).

[244] Report of the Presidential Commission on the Fourth Industrial Revolution, Government Gazette No. 43834, 23 October 2020. Other recommendations contained in the report call for the investment in human capital, establishing an Artificial Intelligence Institute, establishing a platform for advanced manufacturing and new materials, securing and avail data to enable innovation as well as providing incentives for future industries, platforms, and applications of the 4IR technologies amongst others. The report further affirmed the establishment of the 4IR Strategy Implementation Coordination Council in the Presidency. < https://www.gov.za/sites/default/files/gcis_document/202010/43834gen591.pdf. (20 January 2023).

the training of legislators and executives in 4IR and science literacy. This is to ensure that they are able to produce and implement envisaged regulatory changes holistically with agility and capable to compete on a global stage.

It is clear that there is a need for a focused on the regulation, ethics, and cultural aspects for AI to create an enabling policy environment to support private and non-governmental organizations on the ethical and transparent use of new technologies.

Citing research by Centre for Science, Technology and Innovation Indicators in her series of working papers, Alexander argues that most firms are unable or reluctant to use new technologies that tends to violate existing rules.[245] For this reason, an argument was made for the modification of regulations to adapt to new emerging technologies to allow the 4IR to expand in South Africa.[246] It is therefore important to consider that while certain regulations are necessary for AI on the one hand, others would inhibit innovation and creativity on the other hand.

Though the Commission's mandate expired in 2020, the Department of Communications and Digital Technologies has been entrusted with the task of implementing the Presidential Commission (PC4IR) Strategic Implementation Plan.[247] In stark contrast to the recommendations, an implementation plan developed by the Department is silent on how regulatory and legislative measures are going to be realized. However, the

---

[245] Key Opportunities and Challenges for 4IR in South Africa, Rachel Alexander, SARChI Industrial Development Working Paper Series, October 2022. < https://www.uj.ac.za/wp-content/uploads/2021/10/sarchi-wp-2021-08d-alexander-october-2022.pdf. (21 January 2023).

[246] Alexander 2.

[247] PC4IR Strategic Implementation Plan (PC4IR SIP), National Departments Consultation Presentation, March 2021. < https://www.dpme.gov.za/keyfocusareas/Provincial%20Performance%20Publication/Documents/PC4IR%20SIP%20Presentation_National%20Departments%20Consultation%202021.pdf. (21 January 2023).

Plan does more than just to reiterate the Commission's recommendation in terms of recommitting itself to identify impact areas and strategy for regulation, policy and legislative review to create an enabling environment.[248]

The disadvantages of unregulated AI came before the High court in the controversial Telkom case involving the rollout of the radio frequency spectrum, which is critical for 4IR as it enables unfettered access to the internet through open source.[249] This was an application to interdict the Independent Communications Authority of South Africa (ICASA) from issuing licenses for spectrum alleging flawed processes. The process for issuing the licenses was conducted in terms of the 2015 Digital Migration Policy under sections 30 and 31 of the ECA Act which empowers ICASA to manage and grant licensing for far radio frequency in a fair manner without prejudicing anyone.[250]

The applicant, Telkom, argued that the process to grant the licenses was flawed and monopolistic in that it favours only two players in the name of Vodacom and MTN. Based on this, Telkom sought interim relief requiring ICASA to withdraw the invitation to apply for the licenses in question.

In deciding the matter, the court relied on the high court judgement in the Minister of Telecommunication and Postal Services, which highlighted the

---

[248] PC4IR Strategic Implementation Plan 4.

[249] The Minister of Telecommunications and Postal Services v Acting Chair, Independent Communications Authority of South Africa; Cell C (Pty) Ltd v Acting Chair, Independent Communications Authority of South Africa. (2016/59722; 2016/68096) [2016] ZAGPHC 883. <www.saflii.org/za/cases/ZAGPPHC/2016/883.pdf. (22 January 2023).

[250] ICASA is empowered by section 30 of the Act to take overall responsibility in relation to the licensing of the radio frequency spectrum. In doing so it must comply with (s30) (2)(a)) with applicable international standards and requirements for digital electronic communications facilities. In addition, section (31) makes it mandatory for ICASA to prescribe procedures and criteria for awarding radio frequency spectrum licenses for migration from analogue to digital broadcasting fairly without prejudicing any applicants.

inextricable relationship between telecommunication and human rights as follows:[251]

> *"[10] Our everyday experience of telecommunications in the form of radio, television, internet and cellular telephones and so on, is made possible by the service providers utilising a portion of the radio frequency, which exists naturally, to transmit electronic signals. The radio frequency spectrum, like water and electricity is a crucial dimension of social life. Access to the utility of the frequency spectrum implicates the optimal achievement of several constitutional values and rights, including the freedom of trade, modern education and the dissemination of information pursuant to freedom of expression. Achieving effective access to its utility implicate equality too because of its role in facilitating these several rights. The regulatory regime owes, as alluded to earlier, in part, its lineage to The Constitution.*

Against this backdrop, the court find that ICASA did not comply with the provisions of ECA, the Constitution and other statutory obligations. As such, the court concluded that it should not continue with the process of applications for radio frequency spectrum.[252]

The case reflects on the microcosm of challenges that are bound to plague the implementation and regulation of AIS strategies going into the future. As indicated above and despite the absence of a single piece of legislation regulating 4IR and AI in particular, several legislative frameworks are in place, and some are enacted in dribs and drabs targeting specific areas. A number of these laws are discussed below.

5.3 Constitutional and legislative gamut acceptive to AIS

The transformative nature of the Constitution of the Republic of South Africa 1996 (Constitution) appears to be amenable in recognizing the legal status of AIS. Section 8(3) of the Constitution provides that in interpreting

[251] The Minister of Telecommunications and Postal Services para 13.
[252] The Minister of Telecommunications and Postal Services para 55.

the Bill of Rights to a natural or juristic person the courts must develop rules and common law to give effect to a constitutional right and limitations on the proviso that a limitation is in accordance with the provisions of section 36(1).[253] These provisions may open space for the recognition of a non-human business entity.

The provisions in section 8 provides a room to accommodate the legal personality such as of AIS by way of developing common rules and for curtailment of constitutional rights that may be allocated to AIS. Therefore, it could be argued that the courts may resort to sections 8(2) and (3) as well as section 36 of the Constitution.[254] Similarly, the interpretation clause in section 39(2) requires the courts and related bodies to consider international and foreign law when interpreting any legislation to promote the spirit, purpose, and object of the Bill of Rights. Subsection (3) is more interesting in that the Bill of Rights accommodates any other rights conferred by common law or any other legislation provided it is in line with the overall provisions of the Constitution.[255]

The Internet and its sources have now become an essential commodity and occupy a central place in the operation of AIS, in conjunction with the Internet of Things (IoT), generally describe as:

> "the network of physical objects— "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools."[256]

---

[253] See the Constitution of the Republic of South Africa, 1996.
[254] 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, while ss (3) imposes a duty on the courts to apply and develop common law rules subject to the limitation clause contained in section 36(1).
[255] The subsection provides that (3) The Bill of Rights does not deny the existence of any other rights 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.

However, it is not accessible to most people in South Africa, the provision of section 32 of the Constitution provides for the right of access to information held by the state and any person in order to exercise or protect any right.[257] The 4IR is driven by internet connectivity and data infrastructure, which are inextricably linked to the provision of basic services such as health, work, food, education, and personal security amongst others. Given this constitutional framework, the South African courts may have to apply purposive interpretation and be guided by decisions of other jurisdictions when confronted with issues relating to the legal personality of AIS.

In a matter involving pension funds for municipal employees, the SCA in the Natal Joint Municipal Pension Fund case adopted a purposive interpretation of statutes to properly clarify the definition of pensionable emoluments as provided for in the relevant regulations.[258] The court defined statutory interpretation as entailing a process of attributing meaning to the words used in a document, legislation, or some other statutory instruments having regard to the context provided by reading the particular provision or provisions in the light of the document as a whole and the surrounding circumstances. The court went further to illustrate the process and held that:

> The process is objective not subjective. A sensible meaning is to be preferred to one that leads to insensible or unbusinesslike results or undermines the apparent purpose of the document. Judges must be alert to, and guard against, the temptation to substitute what they

---

[256] Friess, Guillemin, Bassi and Doody Internet of things strategic research roadmap. In Internet of things-global technological and societal trends from smart environments and spaces to green ICT at 9 - 52.

[257] Section 32 provides that: (1) Everyone has the right of access to – (a) any information held by state, and (b) any information that is held by another person and is required for the exercise or protection of any right.

[258] Natal Joint Municipal Pension Fund v Endumeni Municipality 2012 4 SA 593 (SCA) para 18.

> regard as reasonable, sensible or businesslike for the words actually used. To do so regarding a statute or statutory instrument is to cross the divide between interpretation and legislation.

The regulatory framework for the financial sector in the banking, insurance, and intermediary is largely self–regulatory and institutionalized from a financial safety and market conduct perspective. To this end, Financial Sector Regulation Act provides for the establishment of the Twin Peaks supervisory model in the form of the Prudential Authority (PA) and Financial Sector Conduct Authority (FSCA) to promote financial stability respectively. The PA is charged with the responsibility ensure the safety and soundness of financial institutions in the interest of customers and the broader public, while the FSCA deals with the conduct of financial institutions and fair treatment of customers, and integrity of the financial market.

The possible use of currency for illegal, money laundering and terrorist activities is regulated through the Prevention of Organised Crime Act 121 of 1998, the Financial Intelligence Centre Act 38 of 2001 and the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004. The South African Reserve Bank is responsible for ensuring that the national payment system complies with existing legislation. These laws regulate functions relating to risks management in relation to audits, credit certifications, and identity verifications amongst others. If left unchecked and monitored, the use of AI systems may pose unimaginable risks paving way for a plethora of criminal activities.

Another interesting development is the recent regulation of cryptocurrencies by the FSCA in a general notice.[259] The FSCA enjoys wide powers conferred in terms of the FIAS Act. The definition of financial

[259] FSCA Press Release, 20 November 2020, FSCA Press Release FSCA publishes a draft Declaration of crypto assets as a financial product 20 November 2020.pdf. (13 December 2022).

products in section 1(h) was used to regulate cryptocurrencies. It is defined as any other product similar in nature to any financial product referred to in paragraphs (a) to (g), inclusive, declared by the registrar by notice in the Gazette to be a financial product for the purposes of this Act.[260]

The definition was therefore used to accommodate and regulate crypto assets, which are defined broadly as digital representation of value not issued by a central bank, but is capable of being traded, transferred, or stored electronically, by natural and legal persons, for the purpose of payment, investment and other forms of utility. It should however be cautioned that this declaration does not mean that recognition of crypto assets means the legal tender representing money issued in terms of South African Reserve Bank Act.[261] Section 17 (1) of this Act defines legal tender only in relation to payments of an amount equal to the amount specified in a banknote or coin, thus ruling out any digital representation of money such as cryptocurrencies in the form of bitcoins amongst others.

This digital representation applies cryptographic techniques by using distributed ledger technology. Until now, crypto assets have not been regulated under South Africa's financial regulations, or otherwise, which has left traders exposed. Therefore, financial regulations in the sector will also be applied *mutatis mutanti* to crypto assets suppliers and trading platforms. Of critical importance is the protection of customers using digital currency while preserving and enhancing the integrity of currency flow in the light of deployment of AIS in the sector. It would seem that developments in the financial and blockchain technology front may offer some glimmer of hope in the conceptualization of the legal personality of AIS.

---

[260] FAIS s 1 (h).
[261] South African Reserve Bank Act 90 of 1989, Section 17 (1).

To put it into perspective, blockchains relate to software decentralized technologies which follow rules of formatting and processing protocols that are expressed in a computer code resulting in the invention of cryptocurrencies.[262] Basic blockchain protocols are able to perform simple functions such as exchanging values for Bitcoin or ownership of digital assets through automated smart contracts to perform complex financial transactions amongst others without human involvement.[263]

Before delving into the legal intricacies of cryptocurrencies, it would be imperative to reflect on legal accountability and liability in the financial and banking sector in South Africa.

5.4 Challenges of corporate governance and accountability

As duties and responsibilities of corporate leadership become more complex and digitized, companies will steadily rely on AIS in their operational and management systems in the foreseeable future. A possibility exists that AIS may have to be explicitly roped in to complement the leadership and managerial hierarchies of companies.

However, legislative bottlenecks contained in the Company's Act may prove to be an impediment to this. To demonstrate this, section 1 of the Companies Act defines a company in three ways. It defines it as a juristic person incorporated in terms of the Act, as a domesticated company and as a juristic person that has registered before a certain period.[264] It is the domesticated part of the definition which raises eyebrows, especially in the light of the role of platform workers and their relationship with multinational

---

[262] Cryptocurrencies are virtual currencies that use decentralized autonomous networks and most popular ones include bitcoin, stellar, polygon, Litecoin and stablecoin amongst others.
[263] Michael Anderson Schillig (2023): Decentralized Autonomous Organizations (DAOs) under English law, Law, and Financial Markets Review, < https://doi.org/10.1080/17521440.2023.2174814. (20 February 2023).
[264] S 1 of the Companies Act 71 2008.

corporates whose most of their operations are mainly online, as indicated in chapter 3 of this study.

In South African terms, the definition of a board, shareholder, and company director contain a personality element in section 1 of the Company's Act. Certainly, AIS are not accommodated in the reference to juristic persons in these provisions. Apart from the legal status of AIS in corporate governance, it would also be critical to consider the legality of delegated or *de jure* directors in corporate settings. While the Companies Act provides for the appointment of proxies, it is also not clear on the validity of the acts committed by *de facto* directors.[265]

Section 58 provides for the right of a shareholder to appoint a proxy, who is entitled to all rights and privileges enjoyed by a shareholder provided due process of appointment was followed. However, the Act is silent on the definition of a proxy and an agent. Applying common law principles, the assumption is that liability arises once such acts or decisions are officially endorsed and adopted by relevant company structures.

Section 5(1) requires that the Companies Act must be interpreted and applied to promote national economy, transparency and high standards of corporate governance. In addition, the Act further requires the balancing of the rights and obligations of shareholders and directors.[266] The requirement for the balancing of these rights and obligations is critical in minimizing biases and boosting independence of company leadership in the event AI is deployed and incorporated in the corporate governance ecosystem.[267] In support of this, Hamadziripi is of the view that:

---

[265] Kilian, N. (2020). Legal Implications relating to being "Entitled to Serve" as a director: A South African-Australian Perspective. *Potchefstroom Electronic Law Journal (PELJ)*, *23*(1), 1-27. https://dx.doi.org/10.17159/1727-3781/2020/v23i0a8174, (20 February 2023).

[266] S 7 of the Companies Act 71 2008.

[267] Hamadziripi and Chitimira "The Integration and Reliance on Technology to Enhance the Independence and Accountability of Company Directors in South Africa" 2021 Potchefstroom Electronic Law Journal 24 at 24.

> the use of augmented AI would enhance the independence of directors since directors with dissenting opinions might be encouraged to contribute their views by simply relying on decision-support AI recommended as the basis of their dissent.[268]

Other provisions having legal implications for AIS relates to the provisions on business judgment rule and exercise of fiduciary duties in section 76(4)(a) and 76 (3)(c) respectively. The provisions imposes obligations on the part of directors to take reasonable and diligent steps to be informed and educated about any matter concerning the operations of a company before a decision is taken. In practical terms, a director must understand and appreciate the technical capabilities of AIS systems in order to fend off any potential harms and losses that may attract legal liabilities. Failure to exercise this critical fiduciary duty would result in being held personally liable. A director can only be protected and exonerated if acted independently in good faith considering the interest of the company.

In South Africa, a company can sue and be sued in its own name or directors individually.[269] In this case, the SCA ruled that shareholders cannot sue company directors for a misleading audit finding which resulted in the devaluation of their shares. The requirements for business judgment rule and the duty to act with care, skill, and diligence present difficulties when liability arises when company directors and board members relied on AIS to arrive at a particular decision.

In a matter concerning the identity and relationship between a municipality and municipal council, the High court in Nelson Mandela Municipality & others dealt with a dispute amongst political parties in a coalition and a municipal council regarding the choice of a municipal manager.[270] As a result, the municipal council, city manager and a mayor applied for interim

---

[268] Hamadziripi 19.

[269] Hlumisa Investment Holdings (RF) Limited v Kirkinis 2019 4 SA 569 (GP).

[270] Nelson Mandela Bay Municipality and others v Qaba and others [2022] JOL 52864 (ECP)

relief to interdict the recently appointed municipal manager from exercising any authority. The municipal manager was appointed by a resolution adopted by a council meeting which was boycotted by other parties in the council.[271]

The central difficulty posed by the case concerns the identity of the parties as to whether it is possible for a municipality to sue its own council.[272] This has proved to be a *sui generis* situation where a municipality sues its own council.

To resolve the matter, firstly the court made reference on the establishment, composition, membership and terms of office for municipal councils as provided for in sections 157, 158 and 159 of the Constitution. Secondly, the court went further to considered section 160 of the constitution to demonstrate that a municipality cannot separately hold power, authority or legal interest from its council.

The court considered section 2 (d) of the Municipal Systems Act which provides that a municipality "has a separate legal personality which excludes liability on the part of its community for the actions of the municipality."[273] While the court regard this as having an effect on incorporating the municipality with a separate legal personality from its community, it found this to be affirming the essential form of incorporating a municipality at local government sphere as it does not contemplate municipality as separate from its council. The court viewed this notion as an absurdity since it is the council in which both the executive and legislative powers and authority are vested.[274]

---

[271] Nelson Mandela Bay Municipality and others para 8.
[272] Nelson Mandela Bay Municipality and others para 16.
[273] Section 2 of the Municipal System Act No. 32 of 2000 provides that: "A municipality – (a) is an organ of state within the local sphere of government exercising legislative and executive authority within a determined area ……..and it consists of – (i) the political structures and administration of the municipality; and (ii) the community of the municipality……. (d) has a separate legal personality which excludes liability on the part of its community for the actions of the municipality."

Based on these findings, the court concluded that the municipality is vested with constitutionally conferred powers and responsibilities in terms of the law consisting of councils elected by the community as integral part of a municipality and as such dismissed the application for interdict considering the requirements of an interim relief.

Considering the substance of the case, despite the fact that the matter relates to state organ, it could be argued that a similar legislative provision can be framed and employed when regulating the legal personality of AI systems as part of ensuring its accountability and liability. Already, the Companies Act does demarcate responsibilities of company directors from that of board of directors when it comes to corporate law.

The matter also becomes more difficult when the decision was solely taken by the AIS. For an example, in 2014 a Hong Kong-based company, Deep Knowledge Venture, appointed an AIS in the name of VITAL (Investment Tool Verification to Advance Life Sciences) to its board of directors on an observer basis.[275] It was granted all the rights enjoyed by other board members including voting rights despite the fact that it does not have the status of directorship as required by the laws in Hong Kong. As the first AI to serve on the board, VITAL was mainly used in taking decisions relating to investments.

The financial sector adopts a fit and proper requirement as a yardstick to determine and meet the requirements in section 6A of the Financial Advisory and Intermediatory Service Act 2002 (FAIS). The provisions provide for the registrar who is enjoined to classify financial service personnel as key individuals, representatives, key individuals, and compliance officers.[276] This classification sound more or less the same as

[274] Nelson Mandela Bay Municipality and others Para 26.

[275] See Eroğlu, and Karatepe, "Impact of Artificial Intelligence on Corporate Board Diversity Policies and Regulations" 2022 European Business Organization Law Review 23 at 541.

the risk classifications in the EU frameworks. However, based on this the registrar is then able to determine the fit and proper requirements in each category.

Amongst others, the determination of fit and proper depends on competency, qualifications, continuous professional development, and experience.[277] While it is clear to apportion liability, it may also turn out to be difficult to identify where fault emanates based on these classifications. It is in this context that the question of eligibility of coopting AIS into corporate governance comes to the picture.

In the course of business, board members often share confidential information amongst themselves using various platforms. They use this for data review, risk management systems, and audit systems. In the financial services sector, AI-based risk-management systems have also been used to perform legal compliance functions like detecting credit card fraud and money laundering. Since the main task of the corporate board is monitoring management, both the information flow to the board as well as risk management are crucial aspects of corporate governance. Thus, AI clearly holds promise if it can help with these important tasks.

In South African context, the provision of financial advice to clients places financial planners under onerous fiducial duty and regulatory obligations, especially in cases where AIS are deployed. The Act defines advice to include “any recommendation, guidance or proposal of a financial nature furnished, by any means or medium, to any client or group of clients”.[278] The Financial Services Board (FSB) grants licenses to financial advisors if they meet the requirements of the Act. In the event such advice is solely based on recommendations by AIS, it would be difficult to apportion

[276] FAIS ss 6A (1) (aa)-(dd).
[277] FAIS s 6A(2)(a)-(d).
[278] FAIS section 1.

liability and ensure a well-deserved compensation is made to victims of harms arising from such advice.

5.5 Regulation and management of data governance

With its myriad past challenges based on discriminatory grounds, South Africa would have to contend to the caution and sensitivity when regulating data mining, collection, and analysis.[279] Data policy and management in South Africa is driven from a designated government department, the Department of Communication and Digital Technology. However, from a practical point of view, data policy is broad and cross-cutting. As such it impacts on other strategic areas whose operations are underpinned by the 4IR technologies such as Industry 4.0, artificial intelligence, biotechnology, and capability building. In addition and across this broad scope, several strategic principles may guide data policy and how it should be managed.

It is in the basis of the transversal nature of these 4IR technologies that South Africa has paid scant attention to regulation of AIS. However, much has been done in terms of regulation and management of data, especially in areas of health, justice and social welfare amongst others.

Indeed, data has become money, real money in which every crook would want to lay their hands on. Various forms of data are critical in ensuring an effective and sustainable artificial intelligence systems. This data is collected or mined in various ways and include personal, health, environmental, trade and economic data amongst others. It is the governance and ownership of these data that makes the AIS a bit controversial especially when it comes to its storage, accessibility, and usage.

[279] Section 9(3) of the Constitution of Republic of South Africa provides for equality and prohibits direct or indirect unfair discrimination on various identified grounds. Amongst others, the ground include race, gender, sex and age to mention but few.

Firstly, most of these data is mined and collected from poorer nation for the benefit of richer nations under the guises of research, foreign investment and public good as a result of massive resources at their disposal. As a result, poor nations easily avail these data to be exploited thus leaving them in a precarious state resulting in compounding digital divide. While developed countries collect this data with ease, sometimes it has proven difficult to share the same data with less developed countries where this data is derived[280].

The race for access to COVID 19 vaccine clearly demonstrated that pharmaceutical companies are more interested in profiteering than the well – being of humanity, especially those from less developed nations.[281] The companies in charge of data resources commands immense power over governments as the collection, capturing and analysis of data involves millions in profit – making. Most of these data is used for socio – economic development, environments, security and health within the context of the SDGs, and are sometimes available on an open source.[282]

As a result, this leaves most of corporate companies in control of massive global that data that can be used good of humanity and equally for nefarious purposes with a potential to violate fundamental and human rights as indicated elsewhere in the study. In the finance sector, this manifest itself through hacking and cybercrimes. Hacking can be described as a technique used to manipulate computer systems to gain unauthorized access to a computer system, data or program targeting both private and public institutions.

---

[280] Coli Ndzabandzaba, Data sharing for sustainable development in less developed and developing countries , Institute for Water Research, Rhodes University, 2018, South Africa* < Microsoft Word - ~5229735 (un.org). (23 March 2023).

[281] Anisha Amarat Jogi, Artificial Intelligence and Healthcare in South Africa: Ethical and Legal Challenges, UNISA, 2021. < https://uir.unisa.ac.za/bitstream/handle/10500/28134/thesis_jogi_aa.pdf?sequence=1&isAllowed=y (23 March 2023).

[282] Big Data for Sustainable Development, UN Global Pulse 2017. < pdf (un.org)Big Data for Sustainable Development | United Nations.(26 March 2023).

On the one hand, hacking is mostly used for malicious purposes of profiteering, blackmailing or just for bragging rights. On the other it is also used for ethical and security reasons, in the interest of the public and governments. Through this process, personal data is accessed and processed for both nefarious and ethical purposes using technological systems. With the predominant use of AIS, the situation becomes more complex, especially when artificial intelligence software evolves into more advanced stages.

In South Africa, POPIA regulates how business and government should handle personal data and provides for remedial sanctions against responsible parties in the event of unlawful access and processing of personal data. However, most interestingly, the Act defines a person to include natural and juristic persons to the exclusion of AIS. Thus, AIS is does not fall into this definition and as such no legal liability and accountability can be attached to it.

The Cybercrimes Act has now been enacted, replacing the ECTA Act while simultaneously reinforcing the POPI Act by providing for more robust protections against cybercrimes.[283] The Cybercrime Act provides regards any person who unlawfully and intentionally happens to access a computer system or computer storage medium to be guilty of an offense[284].

The definitions of access to data, computer programs, and computer storage medium are broadly defined in section 1 of the Act to include espionage and hacking in the corporate sector as crimes. In this context, the data in question includes passwords, codes, pins, access cards, and any device used to access, modify or delete contents in a software program. The definition of unlawful access can be in the form of downloading or saving a file or sending an email to someone. It is

[283] Cybercrime Act 19 2020.
[284] Section 2 (1) of Cybercrime Act 19 2020.

therefore imperative that software engineers, developers, importers, and distributors of hacking software risk being held liable if not careful.

It is clear that the Cybercrimes Act is a welcome development in our legislative landscape as it addresses critical aspects emanating from the deployment of AIS to a particular extent. While the Act criminalizes different types of cybercrimes and attacks, it also serves as a powerful tool to strengthen data protection. The fact that the Act criminalizes unlawful and intentional access to data, computer storage medium, and computer systems, means that corporate companies may also be held accountable in terms of both the Cybercrimes Act and POPIA. The difference between the two is that POPIA operates in relationships between data subjects and responsible parties, while Cybercrimes Act is wide and can be used in different contexts and applies both vertically and horizontally. The contexts in question may relate to industrial espionage, bridging electricity, or even DSTV channels, for instance.

5.6.1 Adjudication of data protection breaches by the courts

The High court in the Myeni case dismissed an appeal by hackers who used software overcoming firewall security enabling them to access login details and passwords used by accounting personnel at a local municipality in contravention of section 86 (1) and (4) the ECTA Act.[285] This resulted in the hackers being able to divert and access about R1.4 million from the municipality's ABSA bank account. The penalties meted against the four accused ranged from two years to fifteen years averaging twenty years in prison.

In a recent High Court case relating to duty of care within the corporate governance space.[286] The curt in Hawarden dealt with a question particular

[285] Section 86 deals with unauthorized access to, interception of, or interference with data subject to the Interception and Monitoring Prohibition Act, 1992 insofar as public safety and interest are concerned.

whether a plaintiff who sustained economic loss may claim liability for pure economic loss arising from what is known as business email compromise (BEC). The plaintiff the defendant negligently omitted to forewarn him to take safety precautions and about the risks associated with BEC when sending an email.

In this case, an immovable property was bought by the plaintiff from the third party seller who in turn appointed the defendant conveyancing attorneys to seal the transaction. After paying the deposit for the property, the plaintiff paid the balance of purchase price amounting to R5 million to the conveyancing attorneys using electronic transfer into what she believed was the attorneys account based on the banking details emailed to her by defendant's employee.

The defendant attorney sent an email to the plaintiff's email account which was hacked by fraudsters who then altered the banking details in an unprotected pdf document to reflect their own bank accounts. This resulted in the funds electronically transferred into the fraudster's bank account and not the attorney's account.

The plaintiff argued that the defendant was aware of the risks associated with BEC before the commission of cybercrime and further that the defendant failed to warn the plaintiff about the known risks before effecting electronic payment, which are prevalent in the conveyancing space. It was also argued that the defendant had control on how banking accounts details are conveyed to the plaintiff such as protecting the pdf document and using multi – channel verification to avert cyber fraud.[287] In determining the issue, the court held tha:

---

[286] Hawarden v Edward Nathan Sonnenberg's Inc (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ) (16 January 2023) <https://www.saflii.org/za/cases/ZAGPJHC/2023/14.pdf. (22 March 2023).
[287] Hawarden 47 & 48.

> a duty of care exists between a purchaser in a conveyancing transaction and the conveyancing attorneys handling the transaction so as to prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking to emails containing sensitive information such as bank account details are not invulnerable to BEC.[288]

The court went further to and held that the risk was foreseeable considering the experience of the conveyancing attorney as well as prior knowledge and inherent risks associated with the BEC. Based on this, the court concluded that the defendant was under a legal duty to guard against such harms from occurring.[289]

Having established factual causation due to negligence resulting in the loss suffered the plaintiff's claim of R5.5 million was upheld with costs and defendant conveyancing attorneys ordered to make good of this. [290]

5.6 Sweeping changes in the financial sector regulation

The regulatory framework for the financial sector in the banking, insurance, and intermediary is largely self–regulatory and institutionalized from a financial safety and market conduct perspective. To this end, Financial Sector Regulation Act provides for the establishment of the Twin Peaks supervisory model in the form of the Prudential Authority (PA) and Financial Sector Conduct Authority (FSCA) to promote financial stability respectively. The PA is charged with the responsibility ensure the safety and soundness of financial institutions in the interest of customers and the broader public, while the FSCA deals with the conduct of financial institutions and fair treatment of customers, and integrity of the financial market.

---

[288] Hawarden 101.
[289] Hawarden 126.
[290] Hawarden 129.

The rise of digital money and may have an effect of reducing cash circulation and requires South African industry and regulators to swiftly assess and regulate it as part of risk mitigation.[291] To this end, the finance industry in South Africa has introduced the QR code standardisation, which will promote interoperability between banks, enable consumers to use a single code to make payments through local bank networks and help reduce the cash in circulation.[292] However, the legal framework will need to be significantly overhauled, regulation adjusted, and financial technology enhanced to deal with the pace of progress. South African

The possible use of currency for illegal, money laundering and terrorist activities is regulated through the Prevention of Organised Crime Act 121 of 1998, the Financial Intelligence Centre Act 38 of 2001 and the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.[293] The South African Reserve Bank is responsible for ensuring that the national payment system complies with existing legislation. These laws regulate functions relating to risks management in relation to audits, credit certifications, and identity verifications amongst others. If left unchecked and monitored, the use of AI systems may pose unimaginable risks paving way for an avalanche of criminal activities.

---

[291] Money Anti – Laundering Integrated Task Force Report 2023: Follow the Money, 22 March 2022. <RE1511150_CROSS PROP Annual Sukuk Report (fic.gov.za) (30 March 2022).

[292]Money Anti – Laundering Integrated Task Force Report 2023.

[293] One of the key functions of FICA, established by the Act, is to monitor and give guidance to accountable institutions and supervisory bodies regarding their performance and compliance with their duties and obligations in terms of this Act as provided for in section 4 (c). In its preamble, the POCA Act introduces measures to combat organized crime, money laundering, and racketeering and imposes obligations to report suspected crime and other matters connected therewith. Section (2) Protection of Constitutional Democracy against Terrorist and Related Activities Act provides that any person who, directly or indirectly using any means, deals or facilitates any transaction or performs any act of suspected crime directly or indirectly is deemed to be guilty of a crime. The provisions of all three pieces of legislation are coughed in broad terms to deal with any tiny matter relating to organized crime, money laundering, and racketeering including those conducted through AIS, especially virtual money.

Another ground-breaking development is the recent regulation of cryptocurrencies by the Financial Sector Conduct Authority in a general notice. The FSCA enjoys wide powers conferred in terms of the FIAS Act. The definition of financial products in section 1 (h) was used to regulate cryptocurrencies. It is defined as any other product similar in nature to any financial product referred to in paragraphs (a) to (g), inclusive, declared by the registrar by notice in the Gazette to be a financial product for the purposes of this Act.[294]

The definition was therefore used to accommodate and regulate crypto assets, which are defined broadly as:[295]

> digital representation of value not issued by a central bank, but is capable of being traded, transferred, or stored electronically, by natural and legal persons, for the purpose of payment, investment, and other forms of utility.

This digital representation applies cryptographic techniques by using distributed ledger technology. Until now, crypto assets have not been regulated under South Africa's financial regulations, or otherwise, which has left traders exposed. Therefore, financial regulations in the sector will also be applied *mutatis mutanti* to crypto assets suppliers and trading platforms. Of critical importance is the protection of customers using digital currency while preserving and enhancing the integrity of currency flow in the light of deployment of AIS in the sector.

The provisions in the Bill clearly demonstrate that the Bill is forward-looking and smells potential dangers that may befall the financial sector due to the increasing deployment of AI systems. The harmonization and consolidation of financial sector laws under one roof may be equated with

---

[294] Section 1 (h) of the Financial Advisory and Intermediatory Services Act 200.
[295] The definition according to the South African Revenue Service. <Crypto Assets and Tax | South African Revenue Service (sars.gov.za) (28 November 2022).

the risk-based approach adopted by the EU in its legislative proposals for AIS.

5.6.1 Smelling a hot coffee in the COFI Bill

The Conduct of Financial Institutions Bill has been introduced as a legal framework aimed at harmonizing and consolidating financial sector laws into one law.[296] The Bill seeks to provide a regulatory framework for the conduct of financial institutions and to protect financial customers. From the reading of the Bill, it could be deduced that the legislature and stakeholders in the sector had smelled the coffee in anticipation of the inevitable increased deployment of AI systems in the financial sector in South Africa.

The COFI Bill marks a departure from rules and regulations-based approach to principles and outcomes-based approach to lessen the burden of conducting business in the sector. The Bill represents a positive move away from technical compliance to achieving specified principles. In practical terms, this entails that instead of setting more rules and regulations, the Bill set principles that define the regulation's intent in a more practical way, which can be equated to the OECD guidelines and principles on AI.

The significance of the Bill can be located in Chapter 6, which seeks to promote fair treatment and protection of financial customers. including by promoting the fair treatment and protection of financial customers by financial institutions. This will be achieved by supporting fair, transparent, and efficient financial markets. This will assist in inculcating trust and confidence in the financial sector, dominated by automation and AIS in particular. Most importantly, the Bill explicitly embraces and supports

[296] The Bill was recently passed in the National Assembly and waiting to be assented to by the President. The law is expected to be implemented in three stages up to 2026.

innovation and the development of sustainable innovative technologies, processes, and practices.

Section 28(1) requires financial institutions to establish and implement oversight mechanisms aimed at approving, monitoring, as well as reviewing the design, development and suitability of its financial products and services on an ongoing basis. These provisions are aimed at preventing a conflict of interest and incentivization of behaviour likely to put financial customers in unfair treatment. The mechanisms are also critical in ensuring objectivity and impartiality. The oversight arrangement envisaged in these provisions relates to the twin-peak regulatory bodies, which could also be responsible for the approval of appropriate AI systems used in the financial sector. The approval processes will also have to determine if such systems meet standards and norms applicable in the sector.

The COFI Bill defines and regulates activities undertaken in the financial sector in one law, regardless of the institution performing the activity. This is set to close gaps in the current legal framework, where some activities that constitute financial services escape regulatory oversight as they do not fit into institutional definitions due to fragmented laws. This will level the regulatory framework and attract customers along the way.

In Hunter v Financial Sector Conduct Authority, the Constitutional court had to deal with a matter relating to the impact of harmonization of regulatory bodies which were regulated in a fragmented manner. The case concerns the investigation in the cancellation project of pension funds administration.[297]

The project came about as a response to a change in the way pension funds operated in South Africa. This entailed a shift from funds that were

[297] Hunter v Financial Sector Conduct Authority and Others, (CCT165/17) [2018] ZACC 31; 2018 (6) SA 348 (CC); 2018 (12) BCLR 1481 (CC).

specific to certain employers, to a general fund for contributions by employees from different employers managed into a central fund. As a result, all the assets, liabilities and members were also transferred to a central fund. However, the employer - specific funds were left registered despite the fact that they had become defunct. In 2007, the FSCA started a project to cancel the registrations of defunct funds.

Realizing teething problems implicit in the project, Ms Hunter as a former member of the FSCA orchestrated investigations aimed at stopping the cancellation project. Various investigations were conducted to test the validity of her complain but nothing substantial came out. The legal question at issue was whether the FSCA had a constitutional duty to investigate potentially unlawful cancellations, and whether the FSCA should be ordered to conduct further investigations into the cancellations project.

In determining issues, the court find solace in the Khumalo case dealing with investigative duty and emphasised that the duty requires public functionaries like the FSCA to investigate instances where they might have acted unlawfully. The court acknowledged that not all such instances of potential impropriety are equal and as such, any investigation must be proportionate to the evidence of unlawful action and the seriousness of alleged unlawfulness. As a result, the court ruled that the FSCA had a constitutional duty to thoroughly investigate all the allegations surrounding the cancellation project. However, the court ruled that Ms. Hunter should have used legality principles to review the decision of the FSCA.

The Bill identifies key conduct themes and standards for companies operating in the finance industry as part of protecting customers. To realize this, the FSCA is set to develop a cross-sector code of conduct in the finance industry, which may be supplemented from time to time. As part of enforcement measures, the Financial Sector Regulation Act of

2017 establishing the FSCA, also make provision for the setting up and functions of the Financial Service Tribunal.[298] The Tribunal deals with complaints from the public and inter – partes within the sector, and one of these relates to the complaint of Medihelp Medical Scheme v Registrar of Medical Schemes in 2020.

The matter arose following the institution of investigations into double debiting of funds from medical schemes by both the Registrar of the Council for Medical Schemes and an audit firm it appointed to conduct investigations. The medical schemes lodged an application for reconsideration with the Tribunal expressing discontent in accordance with section 230 of Financial Sector Regulation 9 of 2017 (FRSA).[299] This was disputed and opposed by the Council, arguing that internal remedies must be exhausted first. This despite the fact that the FRSA and its structures are not regulated under the Council.

In determining whether the decision by the Registrar requiring the medical schemes to pay fees for audit firms constituted a decision by a financial sector regulator, the Tribunal found that only relevant decisions may be subjected to reconsideration and that reference to financial sector regulator would be the Council thus excluding the Registrar. As a result, the Council was regarded as a financial sector regulator by virtue of its supplementary functions of information gathering, supervisory on-site inspections and investigations.

The Tribunal found it unlikely that the Legislature intended that the Registrar could be subject to two administrative 'appeals' under different

---

[298] Deidre Phillips, Financial Services Tribunal decision on its jurisdiction over decisions by the Registrar of Medical Schemes, 20 July 2020. < Financial Services Tribunal decision on its jurisdiction over decisions by the Registrar of Medical Schemes - Bowmans (bowmanslaw.com). (19 November 2022).

[299] Section 230 of FSRA provides that 'any person who is unhappy with a decision made by a decision-maker may apply to the Tribunal to reconsider the decision'.

pieces of legislation (the MSA and the FSRA) while fulfilling the same function.

The FSCA and PA are currently working on a regulatory framework and standards which include information technology governance and risk management. The central issues addressed by this framework are cyber security, cyber resilience, illicit financial flows, cloud computing, and outsourcing of IT functions.

5.7 Implications for deployment of automated contracts unpinned by AIS

The deployment of AIS in risk management, credit checks, and *e*contracts may result in biases and discrimination on any grounds set out in the equality provisions in section 9 (3) of the constitution. Section 1 of ECTA defines automated transaction "as an electronic transaction conducted or performed by means of data messages in which a natural person in the ordinary course of business or employment does not review the conduct or data messages".

An increasing number of companies in the financial service sector are using automated transactions to conclude contracts and assess credit profiles amongst others. People from disadvantaged backgrounds, including women and people with disabilities, are susceptible to be disadvantaged by the usage of these systems. This usually happens in cases involving credit applications resulting in discrimination against certain races, women and people with disabilities. Concerns around accountability and transparency in the black box. Similarly, a competent professional may also be disadvantaged if background checks and vetting processes are conducted using AI systems that are algorithmically compromised.

On the side of corporate governance, the deployment of AIS will reduce employee workload or overhead costs through automation thus significantly increasing profits for the business. AIS can also be used to monitor and analyse market and investment trends to assist company operations to maximise profits and grow.

Therefore, if the board does not keep abreast of such technological developments, then it is not being materially informed to effectively govern the corporation and discharging and fulfilling its duty of care. It is imperative for board members to continually keep abreast with new AI developments. For example, the use of defective robo – advisors at the stock exchange that report gains instead of losses may result with negative impact on investors.

The use of automated chatboxes has become prominent in retail contracts and this may result in placing consumers in a worst position than they were before. The Consumer Protection Act may also come in handy in situations of this nature. The makes a provision for a strict and no-fault presumption for legal liability involving the supply of goods and services for any harm arising from product defect and failure and the binding nature of automated contracts in Section 20(c). The Act also places liability on programmers for automated transactions, unless there is proof that deviation from normal programming protocols took place when the automated contracts were concluded.

In a labour matter concerning strict liability, after an interview, the applicant in Jafta v Ezemvelo KZN Wildlife was offered a job through an email.[300] After the laptop crashed while he was replying to the offer, he went to an internet café and managed to reply by accepting the job offer. Unbeknown to him, the email did not go through to be received by the

[300] Jafta v Ezemvelo KZN Wildlife 2008 ZALC 84 (hereinafter referred to as Jafta v Ezemvelo KZN Wildlife).

respondent company. An SMS was then sent to the applicant advising him about the consequences of not replying to an email sent earlier on. The applicant replied to this SMS and equally accepted the offer using the same communication channel.

The question before the court was whether the applicant accepted the job offer despite having used a different channel. In determining the issues, the Labour court applied section 23 of ECTA, which incorporated the common law principles of reception theory. Section 23 relates to the time and place of communications as well as the dispatching and reception of data messages and provides that:

> A data message- (a) used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or……. (b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee…. (c) must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

Under the circumstances, the reception theory only dictates that an acceptance message must be at the disposal of the offeror in contract law. The implication of this is that data messages are considered to have been received in the inbox even if it did not come to the knowledge of the addressee.[301] The mere capability of retrieval is enough to attract legal effect.

[301] ECTA s 23.

Unfortunately, this was not the case in this case, the applicant's email did not reach the respondence email. For this reason, the court ruled that the respondent could not have received the email accepting the job offer in the light of the provisions in section 23 with respect to email communication. However, the court arrived at the conclusion that a valid contact of employed has been created as a result of the SMS sent by the applicant.

6. Conclusion

In South Africa, despite the fact that there is no single legislative framework harmonising the regulation of the legal personality of AIS, a fairly solid base has been laid to cope and manage actions and conduct emanating from the deployment AIS. With a measurable leverage, regulatory bodies in the finance and banking sector have been able to rise to the occasion and develop regulations to level the playing field.

Most companies in the financial and banking sectors are already deploying AIS in their variegated forms in their business operations. Due to their strategic location in the sector, they use these systems in servicing both their customers and clients in the name of efficiency and effectiveness. Equally, corporate management in the sector also uses AIS as support systems for decision–making at both management and board levels. Currently the systems are used as a guide to arrive at particular decisions that would enhance business productivity and profitability.

South Africa will have to be innovative and creative in developing and adapting existing AI legal principles to remain relevant and competitive in a highly globalized economy.

CHAPTER 6: Conclusion, findings, and recommendations

6.1 Introduction

The usage and deployment of AI systems are bound to dominate every aspect of life as the world tithers on the cusp of the 4IR. The international community is faced with two choices, to legislate or let self–regulation take its course. Equally, both routes have their advantages and disadvantages. Given its propensity to harm while bringing in incentives for the benefit of humanity, a careful approach to legislating it seems to be the option the international community needs to consider.

In today's world, a mere click on a technological device may sound more like signing away all your entitlements. If not managed well, data collection methods and mechanisms require an urgent careful approach. Most of the global data for AI takes place in the developed world given their proximity and access to technological aid. Because algorithmic data for AI is sentient and susceptible to subliminal biases, it becomes imperative that the international community intervene urgently and regulate. Failure to act accordingly may as well result in reversing significant progress made especially in terms of human rights as well as the development of humanity.

The international human rights regime plays a pivotal role in balancing the power between individuals and the state. These rights serve as a foundational value for a democratic and open society. The protection and defence of fundamental human rights is also a springboard for the enjoyment of the sanctity of humankind and its concomitant development and well-being, both online and offline dominated by a growing algorithmic and data-driven society. With the 4IR in our midst, it would therefore seem probable and unavoidable that we are headed for the emergence of new strands of fundamental and human right.

6.2 Findings and recommendations

In this section, the study thrashes out pertinent findings and observations uncovered in the course of the study and further outlines recommendations that can be considered in the conception and regulatory frameworks for AIS. The findings and recommendations take into account continuing regulatory, legislative, and policy-making process as it obtains in both the EU and South Africa.

6.2.1 Definition and legal status of AI systems

Observations and findings

From the discussions above, it can be observed that there have been numerous attempts to define the concept of Artificial Intelligence Systems, from both the public and private sector, with a hopeful view that it would be brought under the parameters of a legal person, with legal rights and duties. However, most of these definitions have fallen short befitting to confer such rights and duties. In the main, the need to provide space for innovation and unfettered development of AI systems coupled with reasons of failure by a significant number of global players and states contributed in delaying efforts towards defining these advanced and sophisticated systems. Despite defining AI in a wide scope, it is clear that there is a missing definition of AIS in the literature.

While the EU has taken practical steps to regulate the systems, South Africa has taken no concrete steps to manage and regulate them. By conferring these rights and duties, lines of accountability and liability would have been clarified. It also is clear that attempts taken by the EU to legislate serves as a good starting point in ensuring that development of AIS is ethically sound, legally acceptable, socially equitable, and environmentally sustainable, with an ultimate aim of supporting the economy, society, and the environment.

Recommendations

Having made these observations and finding, it would be feasible to maintain the status quo to exhaust existing legislative and regulatory frameworks in resolving legal issues stemming from the legal personhood of AIS. It seems these frameworks are capable are able to stand the test of time. In the event they become shaky, our court systems and other regulatory bodies should be given the leverage to exercise discretion and develop the law.

Alternatively, the second option could be to assess each risk category system of AI and partly confer certain degrees of limited legal personality status. This could be the case with regard to Decentralized Autonomous Organizations which have assumed some pseudo – personality status comparable to a natural person.

6.2.2 Regulatory approaches

Observations and findings

The approach adopted by the EU on AI governance revolves around a single legislative instrument aimed at harmonizing existing laws in member states. In doing so, it groups and classifies AI applications into four risk categories with a defined set of regulatory tools each. Depending on risk levels, the tools include subjecting certain categories banning, pre – and post–market requirements, transparency requirement, and voluntary measure.[302]

These various risks categories are further subjected to risk management systems which include the furnishing of documentation with adequate descriptions as well as monitoring reporting requirements.[303] However, it is observed that the monitoring and reporting obligations seems to be limited only to designers, developers, producers, and other users of AI systems in accordance with risk levels of each category.

It has also been observed that the EU often employs the precautionary principle when designing regulations and legislation, such as the AI Act.[304] Conversely, the United States habitually embraces the notion of permissionless innovation as opposed to a precautionary approach which elevates AI systems in high regard thus limiting the enjoyment of their benefits by society.

Recommendations

To this end, it is submitted that the notion of reporting and monitoring should also include researchers and related stakeholders. This can take place especially before AIS come into the market, with more focus on documentation, potential problems and harms as well as discursive statements around logic behind decisions by AI systems.

---

[302] For instance, applications relating to social scoring and biometrics categorized as Unacceptable Risks are totally banned, while High Risks applications posing threats to safety or fundamental rights requires pre – and post–market requirements. Limited Risks applications such as chatbots and data collection are expected to satisfy transparency requirements, other Minimal Risks AI applications have the option to be subjected to voluntary measures.

[303] Amongst others, reporting and monitoring obligations are provided for in the EU Proposal Article 67. The high-risk AI systems should have a CE marking showing they are conforming with regulations and are allowed to enter the internal market.

[304] World Commission on the Ethics of Scientific Knowledge and Technology, UNESCO, The Precautionary Principle, 2005.<Results - UNESCO Digital Library (12 October 2022).

Regarding precautionary and permissionless approach in legislating, it is recommended that a precautionary approach over a permissive approach should be adopted when legislating so as to discourage excessive risk-taking by developers when building AI systems. Therefore, a risk-based approach, as adopted in the EU, is necessary for regulating AI.

It is further recommended that South Africa should also adopt a risk – based approach when regulating AIS to ensure accountability and clear lines of liability. In both EU and South Africa, it is submitted that both developers and regulatory bodies conduct their own assessment tools before AIS are brought into the market.

6.2.3 Management and regulation of data governance

Observations and findings

While the introduction of Cybercrimes Act is a welcome development in our legislative landscape in terms of addressing critical aspects emanating from the deployment of AIS, it falls short in describing the usage of advanced software of artificial intelligence systems that are already accessing and processing personal data. While the Act criminalizes different types of cybercrimes and attacks, it also serves as a powerful tool to strengthen data protection.

The fact that the Act criminalizes unlawful and intentional access to data, computer storage medium, and computer systems, means that corporate companies may also be held accountable in terms of both the Cybercrimes Act and POPIA. The difference between the two is that POPIA operates in relationships between data subjects and responsible parties, while Cybercrimes Act is wide and can be used in different contexts and applies both vertically and horizontally. The contexts in question may relate to industrial espionage, bridging electricity, or even DSTV channels, for instance.

Secondly, it has been observed that companies in charge of data resources commands immense power over governments as the collection, capturing and analysis of data involves millions in profit – making. Most of these data is used for socio – economic development, environments, security and health within the context of the SDGs, and are sometimes available on an open source.[305] As a result this leaves most of corporate

companies in control of massive global that data that can be used good of humanity and equally for nefarious purposes with a potential to violate fundamental and human rights as indicated elsewhere in the study.

Recommendations

While South Africa has developed a significant legislative framework regulating data governance and management, much is still need to sufficiently regulate data misuse and manipulation by emerging platform and virtual corporate companies.

Considering the fact that data has become a commodity which will be driving international and domestic corporate companies, withing the parameters of international trade, it would be important to recommend that the international community develop and establish a framework regulating data flows across the border. While this would ensure fair international trade, it would also reinforce the need to combat notions of algorithmic discrimination and transparency.

In the light of this, South Africa should also put in place robust data regulatory framework that would balance public and private ownership of databanks. While this will go a long way in preserving and enhancing socio – economic prospects of the country, it would also reinforce existing frameworks aimed at combating cybercrimes.

6.2.4 Corporate governance and emergence of new business entities

Observations and findings

It has been observed that centuries ago, companies, as non–natural persons, were incorporated to acquire legal status enabling them to hold assets, enter into contracts as well as being able to sue and be sued. Most importantly, company shareholders are not held responsible for the actions of the company as they are regarded as separate entities.

In this regard, a finding is made that, most recently, the DAOs (decentralised autonomous organizations) using smart contracts have extended the analysis of the nature of entities with legal personality in ways that mean that there is now a scope to extend this further to

[305] The World Bank Open Data Bank. < World Bank Open Data | Data. (24 February 2023).

algorithmic-driven AISs. Alongside this, questions of responsibility for the acts and omissions of an algorithm will need to be considered. While it is conceivable that policymakers may permit algorithms to have legal personality, this will only be the case initially if a person responsible for financial and non-financial losses is identified in every case.

Recommendations

It has become more critical that the legal status of algorithms must be viewed in the same manner in which the incorporation of companies to attain legal personhood has evolved over time.

It is therefore recommended that rules of incorporating companies should be changed to bring into the fold incorporated and other entities with varying degrees of liability taking into account levels of shareholding in the entities.

Another example could be for the South African Law Commission should consider reviewing and reforming the Companies Act 71 2008 to include the definition of a ‘board member’, ‘shareholder’, ‘agent’ and ‘proxy’ to be in line with the role of AIS in corporate governance. And also, The Presidential Commission on AI, together with the Department of Justice and South African Law Commission should strengthen research into the investigation of the possibility of conferring legal personhood to AIS and their legal liability.

6.2.5 Technical requirements, standardization and quality assurance

Observations and findings

While the notion of AIS implies complementing or even substituting human skills and expertise, many people may not entirely appreciate how it functions and its impactful effect. What is important is that the wider public would need to be assured of their reliability and safety by producers of AI systems.

To this extent, it would be imperative that producers and developers of AIS would have to be certificated and permits issued especially in areas of high risks such as facial recognition, recruitment, credit application, and healthcare amongst others. The certification and issuing of permits would have to be in tandem with particular standards set for diverse AI systems taking into account trade and social norms in various settings. It should

however be stressed that certification should not be viewed as a substitute for accountability, but instead, complement existing accountability structures and procedures such as disclaimers and remedial processes.

The definition of the concept of ‘essential requirements’ for each risk tier in the EU AI Act is defined in a manner which places different constraints on each risk category. In this way, it implies that different technical standards and mandatory requirements have to be met by designers and developers alike, as would be required by quality assurance and standard setting bodies in the EU.

A finding is also made that larger parts of the corporate sector have developed self – regulatory ethical principles, fortified by existing soft law as part of industry guidelines aimed at achieving secure and ethical AI approaches. This is also supplemented by co-regulatory structures, such as certification schemes and professional rules. This is exemplified by the International Standards Organisation which serves to reinforce technical guidelines by way of referencing that a system, for example, prescribes to reliable technical procedures.

Recommendations

It is submitted that industry standards are introduced and adopted to guide the designing, development, and deployment of AIS. These standards should be geared at employing technological and scientific methods that support ethically acceptable behaviour.

These standards could be used as part of quality control and assurance to respond not only to industrial and commercial practices but also to broader societal and community expectations. Critical to these would be designing, development, and access to system coding, thus making sure that technology design standards address transparency and accountability concerns.

Another critical consideration for certification and accreditation would be compliance with AI Ethical Principles already endorsed by an avalanche of professional bodies and business organizations as part of self–regulation encapsulating soft law. This would reinforce regulatory and policy development which are geared toward establishing competency and agility for AIS. Such regulatory and policy frameworks should be able to delineate responsibilities and liabilities as to who should be held

accountable between the company designing the medical program and a medical practitioner performing a medical procedure using AI systems.

6.2.6 Opacity and transparency challenges

Observation and findings

It has been observed that the while inner workings and the interactions between the components of an AI system may be more opaque and easier to acquire, its coding may often be subjected to the rigours of intellectual property law. As a result, critical features underlying an AI system's operation may become non – obvious and thus not susceptible to reverse engineering.

Since the design, modification, and incorporation of the components of AIS involves multiple individual and firms, it makes it difficult to point out exact party responsible for any harm that may be committed. It is highly possible that some components may have been designed ages ago and also that a designer may not have foreseen that their designs would be used and incorporated into the AIS that would cause harm. With AIS anyone with access to modern smartphones and computer software can compose a computer code from anywhere in the world without the privileges of a resourceful large corporation.

Recommendations

Since it would be unfair to apportion blame component designers whose work is far removed in the completion and operation of AIS due to space and time, the conception of any regulatory and legislative pieces must take into account the following:

- Try to ensure an efficient disclosure of information, particularly where there are differences in terms of time and geographic locations between stakeholders involved in the development and production of AIS.
- Ensure effective protection of user's intellectual property and also encourage innovation and deployment of AI systems in a more equitable manner.

6.2.7 Liability and accountability constraints

Observations and findings

A solid observation has been made about the existence of a well-established product liability regimes in both South Africa and the EU. However, there have been difficulties in regard to legal issues arising from software and hardware infrastructure insofar as AI liability is concerned. Another difficulty is centred on whether a software should be considered to fall within the notion of 'product'. One of the requirements for product liability is its characterisation of a product as a tangible thing.

While the software and the hardware may originate from different companies, software components integrated into a hardware programme are deemed to be a product. Therefore, consideration of a software as a product determines liability of a software manufacture together with a hardware manufacture. On its own, a 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 exist as to whether it should be treated and determined in terms of applicable product liability regime.

Apart from autonomy which encompasses foreseeability problems, AIS also poses risks of control. Human control of machines that are programmed with considerable autonomy is bound to be difficult and this may result in loss of control, malfunctioning, flawed programming, corrupted file, or damage to input equipment amongst others.

Possibility exists that by learning the environment and improving its performance, it may be difficult to regain its control once lost and this may have catastrophic and existential risk consequences to humanity.[306] This is only dependent on the ability of AIS to improve its hardware and software programming to the extent of surpassing human consciousness and cognitive abilities.[307]

Recommendations

Given the fact that distinction between tangible and intangible object becomes more blurred as we enter the 4IR dominated by digital content, it

[306] S Akash, AI, the Biggest Existential Threat to Humankind says Elon Musk, Analytics Insight,14 July 2021. <AI, the Biggest Existential Threat to Humankind says Elon Musk (analyticsinsight.net). (18 January 2023).

[307] 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". Eva Hamrud, AI Is Not Actually an Existential Threat to Humanity, Scientists Say, 11 April 2021.< AI Is Not Actually an Existential Threat to Humanity, Scientists Say: Science Alert. (18 January 2023).

is submitted that, in the medium to long term, a common liability regime for AIS should be developed to bring certain aspect of software within the product liability fold.

6.2.8 Emergence and protection of new fundamental rights

Observations and findings

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 AIS, existing international instruments appears to withstand new threats to human and fundamental rights posed by the 4IR era.

From the study it could be observed that new technologies are bound to have an adverse impact on existing human and fundamental rights on the one hand, and on the other hand have a potential to give rise to new rights. It is therefore clear that most of these potential rights would not be able to be accommodated by existing legislative and regulatory frameworks.

The negative impact of these technologies can be seen through the violation of rights, conflicting rights and new issues all emanating from usage and deployment of new technologies.

Conflicting rights may also arise in instances when 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 study finds that the interpretation and application of existing legal and regulatory frameworks may be overstretched and as a result yields untenable distortions which may drift away from how the rights were originally conceived leading into legal uncertainty and possible infringement of legal protected rights.

Recommendations

It therefore 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 AIS and its implications for human and fundamental rights.

The international community should also ensure that existing efforts to regulate international trade and copyright laws does not disadvantage developing countries. There must therefore be aimed at ensuring equitable access to the benefits of AIS, inasmuch as it is expected that there should be collective approach in confronting challenges posed by the 4IR and AIS in particular.

6.2.9 Development and conceptualization of relevant legislative frameworks

Observations and findings

Against the backdrop of the discussion, it is clear that responsible authorities at all levels should ensure that data collection processes are democratic, transparent, and accountable with the view of eliminating any form of discrimination, biases, and prejudice. There is need to ensure that internet connectivity is a basic commodity which must be freely accessible and provided to everyone.

It has also been discovered that a significant number of existing laws need to be revamped and adapted to conditions and environment for conducive deployment and operations and AIS. This will ensure that there is investor and business certainty in our laws, while also encouraging responsible use of AIS.

Recommendations

The law reform commission should consider reviewing the Companies Act 71 2008 to include the definition of a ‘board member’, ‘shareholder’, ‘agent’ and ‘proxy’ to be in line with the role of AIS in corporate governance. And also, The Presidential Commission on AI, together with the Department of Justice and South African Law Commission should strengthen research into the investigation of the possibility of conferring legal personhood to AIS and their legal liability.

South Africa should consider clustering various economic sectors, like the financial sector, in order to properly regulate and manage the introduction of AIS in a concerted manner.

The government should consider establishing a public liability company to deal with all the liability claims emanating from harms caused by AIS.

6.2.10 Assessment of AI regulation in South Africa

Observations and findings

The has been able to establish that while AI regulation in South Africa is lagging behind, there are steady strides to catch up with the international community to an extend that it is a bit behind the EU. The difference with between the two is that the EU has established a specific legal framework attempting to consolidate existing laws, while South Africa continues to operate on a fragmented pieces of legislative framework especially in the finance and banking sector.

It has also been observed that the Conduct of Financial Institutions Bill has been introduced as a legal framework aimed at harmonizing and consolidating financial sector laws into one law.[308] The Bill seeks to provide a regulatory framework for the conduct of financial institutions and to protect financial customers.

Similarly, the Financial Sector Regulation Act provides for the establishment of the Twin Peaks supervisory model in the form of the Prudential Authority (PA) and Financial Sector Conduct Authority (FSCA) to promote financial stability respectively. The PA is charged with the responsibility ensure the safety and soundness of financial institutions in the interest of customers and the broader public, while the FSCA deals with the conduct of financial institutions and fair treatment of customers, and integrity of the financial market. This will go a long ways to ensure that regulatory bodies within the sector are unified and consolidated for efficiency and effectiveness.

Despite the establishment of the PC4IR with specific mandate in identifying challenges posed by the 4IR and AIS, there is inadequate reference to efforts and plans to set up mechanisms aimed at working on legislative frameworks in anticipation of the 4IR.

Recommendations

Against this backdrop, it is recommended that, after having established a relevant body, South Africa should prioritize harmonization of existing laws for AIS in a holistic manner.

---

[308] The Bill was recently passed in the National Assembly and waiting to be assented by the President. It is expected that the law will be implemented in three stages up to 2026.

It is also recommended that South Africa should begin to kick – start processes aimed at developing a single legislative frameworks for the regulation of AIS. The envisaged legislation would broadly regulate the systems and serve as a frame of reference for other laws that maybe developed specifically to deal with different categories of AIS.

6.3 Conclusion

The words uttered by John McCarthy nearly 70 years ago, on the inability to define AI, have remained uncontested as the systems continuous to be undefined. However, the reasons that existed at the time have now changed and yet there is no unified definition of AIS. Lack or absence of this definition deprives AIS of the opportunity to be conferred with a fitting legal status to enable it to exercise potential rights and duties within the parameters of the law. This, despite the fact that AIS are able to perform tasks and duties comparable to humans, and possibly exceeding humanity going to the future.

The discussion traced the origin as well as subjective and objective intelligence of AI, informed by its theoretical and philosophical underpinnings. The ability of AI to process data, information, letters, characters, and symbols expressed in coding in accordance with a set of instructions held in its memory was also evaluated. From the discussion, it is clear that AI is a multi–disciplinary subject rooted in the study of algorithms and big data structures using its technique from queuing theory, statistics, and probability through hypothesis, testing, and experimentation for its effectiveness.

The distinction between narrow and general AI demonstrates the extent of capability and as a yardstick possibly to be used to measure apportionment of liability and accountability when regulatory frameworks are put in place. While the discussion further places data mining and collection as key determinants of the sociological basis of the algorithm make–up, it also raises questions on issues of data justice and transparency.

As autonomous systems, corporate companies and public sector have embraced these technologies either as aids or substitute to human labour and overall productivity in a quest to maximise profits and provision of services to their clientele and the public in general.

Having cast our eyes beyond South Africa, the study focuses on AI development and regulation in the European Union. Despite existing legislative framework in both South Africa and the European Union, the uncertainty surrounding the legal status of AIS tends to be an albatross over the shoulders of corporate entities to conduct business with ease. Complex lines of liability and accountability between corporate companies and AIS have remained a bone of contention, only to be contested and resolved by regulatory bodies and the courts.

Similarly, new forms of business entities such as DAOS have emerged and seems to the only viable option to be regulated setting out clear lines of liability and accountability. Failure to regulate this would encourage these kinds of entities to independently self – regulate themselves.

Closely related to these, are AIS that are able to generate, invent and create their own intellectual property rights. Continued lack of transparency and accountability by developers and regulatory regimes relating to intellectual property rights powered by AIS does not augur well with the expectation and dictates of a society dominated by artificial intelligence technologies. The development, production, and distribution of AI technologies must be underpinned by principles of accessibility, explainability, openness, and transparency if multi-national corporates are to be held accountable.[309]

Although the EU proposal is limited in scope, it is important to note that these are far-reaching and practically very relevant legislative interventions. Moreover, the proposal also evaluates the directive and envisages further instruments should the evaluation deem additional measures necessary, especially on no–fault rules.

The adoption and passing into law of the EU proposals marks the beginning of the legislative process. The European Parliament and the Council will examine the proposals thoroughly for defining their respective positions. A political agreement, which will be the basis for the formal adoption of the directives by the co-legislators, may well require amendments and compromises in the course of the discussions, with the AI Act being discussed intensively in parallel. If and when adopted, the member states will have some time to implement the directives.

---

[309] Veda C. Storey, Roman Lukyanenko, Wolfgang Maas's, and Jeffrey Parsons. 2022. Explainable AI. Com, 4 (April 2022), 27–29. <https://doi.org/10.1145/3490699. (17 March 2023).

Yet, companies engaged in AI are well-advised to monitor the further legislative developments thoroughly and implement appropriate risk prevention mechanisms. If adopted as proposed, the directives will set new and claimant-friendly standards for product liability in the case of AI systems, but also in general.

Moreover, even further-reaching amendments are on the horizon: The draft AI Liability Directive suggests a review of the directive within five years after the end of the implementation period. The Commission shall examine whether the objectives were reached and, if necessary, propose further measures for adoption, such as the introduction of harmonized no-fault liability rules for certain AI systems and mandatory insurance for the operation of the AI systems.

The E.U. initiatives on the differentiation between high-risk AI and non-high-risk AI shall only serve as a guideline. Focusing mainly on the riskiness of AI instead of sector-specific applications could be a desirable path. Still, a fostered discussion on a flexible and, at the same time, a determined distinction is advisable.

Bibliography

Articles

Abdellatif, N. An Ethereum bill of lading under the UNCITRAL MLETR. Maastricht Journal of European and Comparative Law, (2020), 27(2), 250–274. <https://doi.org/10.1177/1023263X20904316.(15 April 2022).

Akhtar, Muhammad Shoaib & Feng, Tao. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. EAI Endorsed Transactions on Creative Technologies. < https://eudl.eu/doi/10.4108/eai.23-11-2021.172218. (16 April 2022)

Ameer-Mia, Pienaar and Kekana "South Africa" in Berkowitz M (ed)(2020) AI, Machine Learning and Big Data 2nd ed, Global Legal Group Ltd London

Azoulay A, Towards an Ethics of Artificial Intelligence, New Technologies: Where To, December 2018, Vol 3 & 4, < Towards an Ethics of Artificial Intelligence | United Nations. (14 January 2023)

Channon M, Marson J, THE liability for cybersecurity breaches of connected and autonomous vehicles, Computer Law & Security Review, Volume 43, 2021, 105628, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2021.105628. (17 December 2022)

Chesterman, S. (2020). Artificial Intelligence and The Limits of Legal Personality. *International and Comparative Law Quarterly, 69*(4), ARTIFICIAL INTELLIGENCE AND THE LIMITS OF LEGAL PERSONALITY | International & Comparative Law Quarterly | Cambridge Core. Accessed 20 June 2022

Custers B, New digital rights: Imagining additional fundamental rights for the digital era, Computer Law & Security Review, Volume 44,2022, < New digital rights: Imagining additional fundamental rights for the digital era - ScienceDirect (09 March 2023)

Ebers M, 'Liability for Artificial Intelligence and EU Consumer Law' (2021)2 J Intell Prop Info Tech & Elec Com L 204.<https://heinonline.org/HOL/P?h=hein.journals/jipitec12&i=211 (08 October 2022).

Eroğlu, Karatepe, Impact of Artificial Intelligence on Corporate Board Diversity Policies and Regulations" 2022 European Business Organization Law Review 23 at 541

European Journal of Law and Economics (2021) 51:243–284 <https://doi.org/10.1007/s10657-020-09671-5. (30 June 2022)

Fan, W, Geerts F, Data Currency, Foundations of Data Quality Management. Synthesis Lectures on Data Management. Springer, Cham (2012)., https://doi.org/10.1007/978-3-031-01892-3_6. (20 March 2022)

Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., & De Beer, J. (2020). Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. The African Journal of Information and Communication (AJIC), 26, 1-28. https://doi.org/10.23962/10539/30361. (20 March 2022)

Goertzel, Ben. "Artificial General Intelligence: Concept, State of the Art, and Future Prospects" Journal of Artificial General Intelligence, vol.5, no.1, 2014 1-48. <https://doi.org/10.2478/jagi-2014-0001. (17 April 2022)

Koskela, A, Legal Framework of Copyright in Relation to the Development of Artificial Intell10gence. <https://digikogu.taltech.ee/en/Download/154c619f-f75f-4b44-bd45-b4a0e0ca02ef/Tehisintellektiarendamisegaseotudautoriiguste.pdf. (20 September 2022).

Liu, H, Lin C, 2020. Artificial intelligence and global trade governance: a pluralist agenda. *Harv. Int'l Lj*, *61*, p.407. < https://harvardilj.org/wp-content/uploads/sites/15/61.2-Liu.pdf. (19 February 2023)

Maya C. Jackson, Artificial Intelligence & Algorithmic Bias: The Issues with Technology Reflecting History & Humans, 16 J. Bus. & Tech. L. 299 (2021). < https://digitalcommons.law.umaryland.edu/jbtl/vol16/iss2/5. (18 June 2022).

Michael Anderson Schillig (2023): Decentralized Autonomous Organizations (DAOs) under English law, Law, and Financial Markets Review, < https://doi.org/10.1080/17521440.2023.2174814. (20 February 2023

Nowik P, Electronic personhood for artificial intelligence in the workplace, Computer Law & Security Review, Volume 42,2021, < https://www.sciencedirect.com/science/article/abs/pii/S0267364921000571?via%3Dihub. (08 October 2022).

Singh Rajpurohit D & Rishika S, 'Legal Definition of Artificial Intelligence' (2019) 10 Supremo Amicus 87, OSCOLA 4th ed

Orealy T, What is Narrow, General and Super Artificial Intelligence, 12 May 2017, < https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/.

O'Reilly T, "The great question of the 21st century: Whose black box do you trust?", 13 September 2016, <https://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly/?trk=eml-b2_content_ecosystem_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1. <(30 June 2022.

Reyes, Carla, Emerging Technology's Language Wars: AI and Criminal Justice (2022). Journal of Law & Innovation (2022 Forthcoming), SMU Dedman School of Law Legal Studies Research Paper No. 568, Available at SSRN: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217020 (02 June 2022).

Rosioru F, '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. (29 June 2022.)

Stilgoe, J. How can we know a self-driving car is safe? *Ethics Inf Technol* **23**, 635–647 (2021). <https://doi.org/10.1007/s10676-021-09602-1. (24 December 2022).

Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI: Opening the Black Box or Pandora's Box, Communications of the ACM

Steven M. Bellovin, et. al, "When enough is enough: Location tracking, mosaic theory, and machine learning," NYU Journal of Law and Liberty, 8(2) (2014) 555—628. < https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2379&context=fac_pubs. (Accessed 25 August 2022).

Stowe, A, (2022). Beyond Intellect and Reasoning: A scale for measuring the progression of artificial intelligence systems (AIS) to protect innocent parties in third-party contracts. Page Publishing Inc.

Thaldar D, Naidoo M, (2021) "AI inventorship: The right decision?", *South African Journal of Science*, < AI inventorship: The right decision? | South African Journal of Science (sajs.co.za). (05 August 2022)

Tupay P, Ebers M, Juksaar J & Kohv K, Is European Data Protection Toxic for Innovative AI? An Estonia Perspective (2021) 30 Juridica International 99. <https://0-ww-heinonline-org.ultmillen.ul.ac.za/HOL/Page?public=true&handle=hein.journals/jurdint30&div=16&start_page=99&collection=journals&set_as_cursor=42&men_tab=srchresults. (15 September 2022)

Wróbel I.M. (2022). Artificial intelligence systems and the right to good administration. *Review of European and Comparative Law*, *49*(2), 203–223. https://doi.org/10.31743/recl.13616. Accessed 22 July 2022.

Zhou, Q., Zuley, M., Guo, Y. *et al.* A machine and human reader study on AI diagnosis model safety under attacks of adversarial images. National Communication 12, 7281 (2021). < https://www.nature.com/articles/s41467-021-27577-x.pdf?pdf=button%20sticky. (24 December 2022)

Books

Akhtar, Muhammad Shoaib & Feng, Tao. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. EAI Endorsed

Transactions on Creative Technologies. https://eudl.eu/doi/10.4108/eai.23-11-2021.172218. (16 July 2022)

Benhamou, Yaniv and Ferland, Justine. Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages (February 8, 2020). Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law, <: https://ssrn.com/abstract=3535387. (12 October 2022)

Bussiek, H. Digital Rights are Human Rights, An introduction to the state of affairs and challenges in Africa, April 2022. < https://library.fes.de/pdf-files/bueros/africa-media/19082-20220414.pdf (09 March 2023).

Dempsey James X, Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues, Berkeley Centre for Law & Technology August 10, 2020

De Vries, A, (2018) Bitcoin's Growing Energy Problem, Joule, Volume 2, Issue 5, p. 801-805; Dittmar, L., Praktiknjo, A. (2019) Could Bitcoin emissions push global warming above 2 °c Nature Climate Change, 656-657

Dickson, B. What is Narrow, General, and Super Artificial Intelligence, 12 May 2017 <https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/. (15 June 2022)

Du Plessis, L. An Introduction to Law 3ed (1999) 137 (Juta& Co Ltd, Kenwyn)

Dyevre, A. (2016) The Future of Legal Theory and the Law School of the Future. Cambridge: Intersentia

Ebers M, 'Liability for Artificial Intelligence and EU Consumer Law' (2021)12 J Intell Prop Info Tech & Elec Com L 204. <https://heinonline.org/HOL/P?h=hein.journals/jipitec12&i=211. (08 October 2022)

Festinger, L. (1962) Cognitive dissonance, Scientific American. 207 (4): 93-107

Giles, J. & Emma-Iwuoha A 'South Africa Chapter' in A Bensoussan et al. (1st Ed) Comparative Handbook: Robotic Technologies Law (2016

Hamadziripi and Chitimira "The Integration and Reliance on Technology to Enhance the Independence and Accountability of Company Directors in South Africa" 2021 Potchefstroom Electronic Law Journal

Heathon J, Kruger H, South African Family Law (Paperback, 4th)

Hoerber, T. Weber, G. Cabras I, Artificial intelligence in the European Union Policy, ethics and regulation Inga Ulnicane, 2022, The Routledge Handbook of European Integrations

Hoecke, M. (2011) Which Method(s) for What Kind of Discipline? In Hoecke, M. (ed.) Methodologies of Legal Research. Oxford: Hart. 1–18. DOI: http://dx.doi.org/10.5040/9781472560896.ch-001

Kilian, N. (2020). Legal Implications relating to being "Entitled to Serve" as a director: A South African-Australian Perspective. *Potchefstroom Electronic Law Journal (PELJ)*, *23*(1), 1-27. https://dx.doi.org/10.17159/1727-3781/2020/v23i0a8174, (20 February 2023).

Koroleva, P. Action Plan for a Sustainable Planet in the Digital Age.31 May 2022 < CODES_ActionPlan.pdf (unep.org) (10 March 2023)

Malgieri, Gianclaudio and Custers, Bart, Pricing Privacy – The Right to Know the Value of Your Personal Data (2017)

Mattioli, M. (2014) Disclosing Big Data. Minnesota Law Review, 99(2): 535–584.

McCarthy John. The Philosophy of AI and the AI of Philosophy, 1998. aiphil2.pdf (stanford.edu). (15 June 2022).

Michael Anderson Schillig (2023): Decentralized Autonomous Organizations (DAOs) under English law, Law, and Financial Markets Review, < https://doi.org/10.1080/17521440.2023.2174814. (20 February 2023).

Mayer-schönberger, V. and K. Cukier (2013) Big Data; A Revolution that will Transform How We Live, Work and Think. Boston: Houghton Mifflin Harcourt.

Natarajan, P., Rogers, B., Dixon, E., Christensen, J., Borne, K., Wilkinson, L., and Mohan, Sm2021. *Demystifying AI for the Enterprise: A Playbook for Business Value and Digital*

Pariser, E. (May 2011) The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press 17. Review: The Filter Bubble: What the Internet is Hiding from You by Eli Pariser (escholarship.org). (23 December 2023)

Paweł Nowik, Electronic personhood for artificial intelligence in the workplace, Computer Law & Security Review, Volume 42,2021, https://www.sciencedirect.com/science/article/abs/pii/S0267364921000571?via%3Dihub. (08 October 2022).

Pferpferkorn R, Deepfakes in the Courtroom, Public Interest Law Journal, Vol 29, 2020, Center for Internet and Society, Stanford Law School. < https://siliconflatirons.org/wp-content/uploads/2021/02/Pfefferkorn.pdf. (12 December 2022).

Pinto-Bazurco J F, The Precautionary Principle, October 2020, Earth Negotiations Bulletin. < still-one-earth-precautionary-principle.pdf (iisd.org) (23 October 2022).

Resource Book on TRIPS and Development: An Authoritative and practical guide to the TRIPS Agreement, UNCTAD-ICTSD, < https://unctad.org/system/files/official-document/ictsd2005d1_en.pdf. (15 September 2022).

Richards, N. King, J. (2014) Big Data Ethics. Wake Forest Law Review, 49(2): 393–432

Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI: Opening the Black Box or Pandora's Box Communications of the ACM. 1-6. 10.1145/3490699.

Stuart J. Russel & Peter Norvig, Artificial Intelligence: A Modern Approach, 1034, (3d ed. 2010).

Van Heerden B, Skeleton A at al, Family Law In South Africa (Paperback, 2nd Edition)

Veda C. Storey, Roman Lukyanenko, Wolfgang Maas's, and Jeffrey Parsons. 2022. Explainable AI. Com, 4 (April 2022), 27–29. <https://doi.org/10.1145/3490699. (17 March 2023).

Wróbel, I. M. (2022). Artificial intelligence systems and the right to good administration. Review of European and Comparative Law, 49(2), 203–223. < https://doi.org/10.31743/recl.13616. (12 January 2023).

Case law

South Africa caselaw

Financial Mail v Sage Holdings 1993 (2) SA 451 (A).

Hawarden v Edward Nathan Sonnenberg's Inc (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ) (16 January 2023) <https://www.saflii.org/za/cases/ZAGPJHC/2023/14.pdf. (22 March 2023).

Jafta v Ezemvelo KZN Wildlife 2008 ZALC 84

Hlumisa Investment Holdings (RF) Limited v Kirkinis 2019 4 SA 569 (GP).

Hunter v Financial Sector Conduct Authority and Others (CCT165/17) [2018] ZACC 31; 2018 (6) SA 348 (CC); 2018 (12) BCLR 1481 (CC).

Nelson Mandela Bay Municipality and others v Qaba and others [2022] JOL 52864 (ECP)

Natal Joint Municipal Pension Fund v Endumeni Municipality 2012 4 SA 593 (SCA) para 18.

Nkala v Harmony Gold Mining Company Limited (Treatment Action C mpaign NPC and Sonke Gender Justice NPC Amicus Curiae) 2016 JDR 0881 (GJ).

The Minister of Telecommunications and Postal Services v Acting Chair, Independent Communications Authority of South Africa; Cell C (Pty) Ltd v Acting Chair, Independent Communications Authority of South Africa. (2016/59722; 2016/68096) [2016] ZAGPHC 883. <www.saflii.org/za/cases/ZAGPPHC/2016/883.pdf. (22 January 2023).

Foreign caselaw

BlueCrest Capital Management Limited File No. 3-20162, the US Securities and Exchange Commission delivered judgement on 11 February 2021

Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C: 2016:779.

Case 222/84 Johnston [1986] ECR 1651. See also Case C-97/91 Borelli [1992] ECR I-6313) on implementing Union law.

Chetu, Inc.Vko Gaming, Inc., 261 So. 3d 605 (2019) January. District Court of Appeal of Florida. No.4D18 – 1551. <Chetu, Inc. v. KO Gaming, Inc., 261 So. 3d 605 (2019) | Caselaw Access Project. (28 June 2022).

CJEU – Patrick Breyer v Bundesrepublik Deutschland – C-582/14 < CJEU - Patrick Breyer v Bundesrepublik Deutschland - C-582/14 - GDPR Beetle

(21 December 2022)

Cour de Cassation, Chambre Sociale [Labour Division of the supreme court] October 2, 2001, No. 99-42.942 (Fr.). < https://www.legifrance.gouv.fr/juri/id/JURITEXT000007046161/. (11 October 2022.

District Court Zeeland-West-Brabant, ECLI,28-09-2022 / 10072897 AZ VERZ 22-61 <Rechtbank Zeeland-West-Brabant 28 September 2022, ECLI:NL:RBZWB:2022:5656 (18 June 2022)

European Patents Office, applications EP 18 275 163 and EP 18 275, 174 < https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false. (05 August 2022)

Greek Data Protection Authority, Decision of 20/3/2000, The most iconic DPA decisions on DPOs and what you should take from them (iapp.org) (28 June 2022)).

Liberty & Others v the United Kingdom, judgment 1 July 2008

Maxi Weber and Saravia v. Germany, 29 June 2006

McMillian Schrems v Data Protection Commissioner) 21 July 2000, the European Commission's Decision 2000/520/EC of 26 July 2020) in October 2020. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems | European Data Protection Board (europa.eu) .(15 September 2023)

Planet49, CaseC-673/17 1 October 2019, ECLI:EU:C:2019:801. For the headnotes to this decision see this issue of IIC (n11) < https://doi.org/10.1007/s40319-020-00926-x. (24 December 2022)

R (on the application of Edward Bridges) v Chief Constable of South Wales Police (Respondent) and Secretary of State for the Home Department and the Information Commissioner, the Surveillance Camera Commissioner, and the Police and Crime Commissioner for South Wales (Interested Parties) [2020] EWCA Civ 1058

Sarcuni et al v. bZx DAO et al (S. D. Cal., May 2, 2022 < Sarcuni et al v. bZx DAO et al 3:2022cv00618 | US District Court for the Southern District of California | Justia. (23 January 2023)

Tesla case in the US, Case 5:20-cv-02926-SVK Document 1 Filed 04/28/20

The European Court of Justice (case C-414/16 as of 17 April 2018). < http://www.europeanrights.eu/public/commenti/BRONZINI14-CONTRIBUTO_GORI_NEWSLETTER_DICEMBRE-11_-_Charter_-_Vera_Egenberger_-_Gori.pdf. (21 June 2022).

Tulip Trading Limited v Bitcoin Association For BSV & Ors [2023] EWCA Civ 83 (03 February 2023 < Tulip Trading Limited (A Seychelles Company) v Bitcoin Association For BSV & Ors [2023] EWCA Civ 83 (03 February 2023) (bailii.org). (23 February 2023).

Tomomi Umeda v Tesla Inc "Case No.: 5:20-cv-2926

Conference papers

Medvedeva, M. Vols, M. and Wieling, M. Judicial Decisions of the European Court of Human Rights: Looking into the Crystal Ball (A Paper delivered at a Conference on Empirical Legal Studies in Europe, 31 May – 1 June 2018). (19 June 2023).

Policy Options Framework for the Fourth Industrial Revolution in South Africa, An output of the Human Sciences Research Council, South Africa SA-EU Strategic Partnership Dialogue Conference Disruptive technologies and public policy in the age of the Fourth Industrial Revolution 10 - 12 December 2018 CSIR International Convention Centre, Pretoria. < https://hsrc.ac.za/uploads/pageContent/10155/4IR%20Framework%20Report_Final_lowres.pdf (20 January 2023).

Constitutions

Constitution of Republic of South Africa 108 1996

Dissertations and research papers

Anisha Amarat Jogi, Artificial Intelligence and Healthcare in South Africa: Ethical and Legal Challenges, UNISA, 2021. < https://uir.unisa.ac.za/bitstream/handle/10500/28134/thesis_jogi_aa.pdf?sequence=1&isAllowed=y (23 March 2023).

Alexander, R. Key Opportunities and Challenges for 4IR in South Africa, SARChI Industrial Development Working Paper Series, October 2022. < https://www.uj.ac.za/wp-content/uploads/2021/10/sarchi-wp-2021-08d-alexander-october-2022.pdf. (21 January 2023)

Delfino, R. Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act (February 25, 2019). 88 Fordham L. Rev. Vol. 887 (December 2019), Loyola Law School, Los Angeles Legal Studies Research Paper No. 201908.SSRN: https://ssrn.com/abstract=3341593 or http://dx.doi.org/10.2139/ssrn.3341593. (11 January 2023)

Ndzabandzaba C, Data sharing for sustainable development in less developed and developing countries , Institute for Water Research, Rhodes University, 2018, South Africa* < Microsoft Word - ~5229735 (un.org). (23 March 2023)

Wills, G., van der Berg, S. and Mpeta, B., 2023. Household resource flows and food poverty during South Africa's lockdown: Short-term policy implications for three channels of social protection. <

https://www.uj.ac.za/wp-content/uploads/2021/10/nids_cram-wave-1.pdf (08 March 2023)

Government papers

Deidre Phillips, Financial Services Tribunal decision on its jurisdiction over decisions by the Registrar of Medical Schemes, 20 July 2020. < Financial Services Tribunal decision on its jurisdiction over decisions by the Registrar of Medical Schemes - Bowmans (bowmanslaw.com). (19 November 2022).

FSCA Press Release, 20 November 2020, FSCA Press Release FSCA publishes a draft Declaration of crypto assets as a financial product 20 November 2020.pdf. (13 December 2022).

Government Gazette No 42388, 19 November 2019, Terms of Reference for Appointment of Presidential Commission on the 4th Industrial Revolution. < https://www.gov.za/sites/default/files/gcis_document/201904/42388gen209.pdf.(20 January 2023)

Key Opportunities and Challenges for 4IR in South Africa, Rachel Alexander, SARChI Industrial Development Working Paper Series, October 2022. < https://www.uj.ac.za/wp-content/uploads/2021/10/sarchi-wp-2021-08d-alexander-october-2022.pdf. (21 January 2023)

Money Anti – Laundering Integrated Task Force Report 2023: Follow the Money, 22 March 2022. <RE1511150_CROSS PROP Annual Sukuk Report (fic.gov.za) (30 March 2022).

Money Anti – Laundering Integrated Task Force Report 2023.

PC4IR Strategic Implementation Plan (PC4IR SIP), National Departments Consultation Presentation, March 2021. < https://www.dpme.gov.za/keyfocusareas/Provincial%20Performance%20Publication/Documents/PC4IR%20SIP%20Presentation_National%20Departments%20Consultation%202021.pdf. (21 January 2023).

Report of the Presidential Commission on the Fourth Industrial Revolution, Government Gazette No. 43834, 23 October 2020. <

https://www.gov.za/sites/default/files/gcis_document/202010/43834gen591.pdf. (20 January 2023)

Internet sources

Akash, S. AI, the Biggest Existential Threat to Humankind says Elon Musk, Analytics Insight,14 July 2021. <AI, the Biggest Existential Threat to Humankind says Elon Musk (analyticsinsight.net). (Accessed 18 January 2023).

Asquith, M. Tay Tweets: How far have we come since Tay the twitter bot, 11 October 2018.< Tay Tweets: How Far We've Come Since Tay the Twitter bot (hubtype.com). (12 January2023)

Business and Human Rights Resource Centre, Garment Workers During Covid 19 200805_Union_busting_unfair_dismissals_garment_workers_during_COVID19.pdf (business-humanrights.org). (28 September 2022).

Dickson B, What is Narrow, General, and Super Artificial Intelligence, 12 May 2017 <https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence/. Accessed 15 June 2022.

Forbes Magazine, Why Source Data Is The New Currency For Retailers, Brent Brown, Forbes Technology Council,03 November 2021.< https://www.forbes.com/sites/forbestechcouncil/2021/11/03/why-source-data-is-the-new-currency-for-retailers/?sh=32e0ca855e11.(20 March 2022)

Hamrud, E. AI Is Not Actually an Existential Threat to Humanity, Scientists Say, 11 April 2021.< AI Is Not Actually an Existential Threat to Humanity, Scientists Say: Science Alert. (18 January 2023).

Kathrin Bauwens - Mirjam Erb: https://www.linklaters.com/en/insights/blogs/productliabilitylinksProduct Liability and AI (Part 3): Commission plans to overhaul EU product liability law, 29 September 2022. < https://www.linklaters.com/en/insights/blogs/productliabilitylinks/2022/september/commission-plans-to-overhaul-eu-product-liability-law. (12 October 2022)

Lemon, J. Google thinks Obama is Muslim, 19 January 2017. < Step Feed (12 January 2023.

Osborne Clarke Unfair commercial practices law summary, 03 Jul 2008.< Unfair commercial practices law summary | marketing law (osborneclarke.com). (09 October 2022).

Sctott, M. What's driving Europe's new aggressive stance on tech, 28/10/2019, Politico. < What's driving Europe's new aggressive stance on tech - POLITICO. (12 January 2023).

Subramanian, J. Challenges in Cross Border Data Flows and Data Localization amidst new Regulations, SAP Africa Report Blog,19 January 2022. Challenges in Cross Border Data Flows and Data Localization amidst new Regulations | SAP Blogs. (16 September 2022)

The State of AI2021, 18 December 2021. < https://www.mckinsey.com/capabilities/quantumblack/our-insights/global survey-the-state-of-ai-i n-2021.(16 March 2023)

Veda C. Storey, Roman Lukyanenko, Wolfgang Maas's, and Jeffrey Parsons. 2022. Explainable AI. Com, 4 (April 2022), 27–29. <https://doi.org/10.1145/3490699. (17 March 2023)

Legislation

South AFrica

Artificial Intelligence Act, Securiti https://securiti.ai/eu-artificial-intelligence-act/ (11 October 2022).

Financial Advisory and Intermediatory Services Act 200

South African Reserve Bank Act 90 of 1989, Section 17 (1).

Companies Act 71 2008

Cybercrime Act 19 2020.

Municipal System Act No. 32 of 2000

Local Government: Municipal Demarcation Act

Protection of Constitutional Democracy against Terrorist and Related Activities Act

EU Product Liability Directive

Foreign laws

Biometric Information Privacy Act(740 ILCS 14/) . < https://www.documentcloud.org/documents/6248797-Patel-Facebook-Opinion.html. (15 March 2022).

Danish Consolidate Patents Act 90 2019, The Consolidate Patents Act (Consolidate Act No. 90 of January 29, 2019) (wipo.int). < (11 December 2022

Finnish Patents Act 550 1967 (As amended). Patents Act (Act No. 1967/550 of December 15, 1967, as amended up to Act No. 1995/1695 of December 22, 1995) (wipo.int)

Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads. 2021. Web Page. https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/. (30 June 2022).

German Patent Act 30 2021, Federal Law Gazette, PatG - englisch (gesetze-im-internet.de) (12 December 2023)

Polish Industrial Property Law 30 2000. < Act of June 30, 2000, on Industrial Property Law (as amended up to 2015) (wipo.int). (28 June 2022)
Swedish Patent Act 837 1967 (As amended). < The Swedish Patents Act (wipo.int) (28 June 2022)

UK Patents Act 1977 (As amended). The Patents Act 1977 - GOV.UK (www.gov.uk) (28 June 2022)

International instruments

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs).

Berne Convention for the Protection of Literary and Artistic Works as amended on September 28, 1979

Big Data for Sustainable Development, UN Global Pulse 2017. < pdf (un.org)Big Data for Sustainable Development | United Nations.(26 March 2023

Ethical perspective on science, technology and society: a contribution to the post-2015 agenda, report of COMEST, UNESCO, 2015. < Ethical perspective on science, technology and society: a contribution to the post-2015 agenda, report of COMEST - UNESCO Digital Library. (10 October 2022).

International Covenant on Civil and Political Right, adopted on 16 December 1966

OECD AI Principles were adopted by 40 countries in the west for innovation and trustworthiness in terms of human rights and democratic values by setting standards that are practical and flexible enough to stand the test time. <The OECD Artificial Intelligence (AI) Principles - OECD.AI. (03 July 2022).

OECD's five Principles on AI.< https://oecd.ai/en/ai-principles/. (03 July 2022)

Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies(European Parliament 2020 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html) (hereafter EU Framework Resolution).Also see

European Commission 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN. (29 March 2022)

The European Parliament Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (European Parliament, 16 February 2017)

The United Nations through the World Health Organisation went to great lengths to ensure that the diseases are mitigated and controlled. Some of the guidelines and policy directives are found here <https://www.ohchr.org/en/covid-19/covid-19-guidance. (29 June 2022)

UNCITRAL "UNCITRAL Model Law on Electronic Transferable Records" (United Nations, 2017). < UNCITRAL Model Law on Electronic

Transferable Records (2017) | United Nations Commission On International Trade Law. (15 April 2022)

UNESCO Recommendation on the Ethics of AI, 2022 < Recommendation on the Ethics of Artificial Intelligence - UNESCO Digital Library. (19 September 2022).

World Commission on the Ethics of Scientific Knowledge and Technology, UNESCO, *The Precautionary Principle*, 2005.<Results - UNESCO Digital Library (12 October 2022).

World Intellectual Property Organisation Copyright Treaty (WIPO)

Regional instruments

African Charter came into force on 21 October 1986 and acceded to by South Africa on 09 July 1996.

Council of Europe, Guidelines on addressing the human rights impacts of algorithmic systems", (appendix to Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems)

Council of Europe Convention for the Protection of Individuals regarding Automatic Processing of Personal Data is another source of 49 pan-European data protection obligations binding on all EU Member States.

Council of Europe (2020) Preventing discrimination caused by the use of artificial intelligence. https://ennhri.org/about-nhris/human-rights-based-approach/. (20 June 2022)

Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2002 < Declaration of Principles on Freedom of Expression 2019 | African Commission on Human and Peoples' Rights (au.int). (22 December 2022).

Directive 2009/24/EC of the European Parliament and the council of 23 April 2009 on the legal protection of computer programs [2009] OJ L111

Directive (EU) 2016/680) provides for harmonized rules applicable to the design, development, and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 as amended by Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89 (Law Enforcement Directive), OJ L 119, 4.5.2016, pp. 89-131.

Directive (EU) 2020/1828 of The European Parliament and of The Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020L1828&from=EN. (12 October 2022).

Employment Equality Directive (2000/78/EC),9 the Racial Equality Directive (2000/43/EC)

EU Commission, 2020. Report on the safety and liability implications of Artificial

European Convention of Human Rights

European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)European Declaration on Digital Rights and Principles | Shaping Europe's digital future (europa.eu) (07 March 20230).

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)., paragraph 59.< https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051 (10 October 2022)

Gender Goods and Services Directive (2004/113/ EC)

Gender Equality Directive (2006/54/EC)

General Data Protection Regulations

Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

Proposal for a directive of the European Parliament and of the Council on liability for defective products. < COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective

products | Internal Market, Industry, Entrepreneurship and SMEs (europa.eu) as well as COM(2022) 496 final 2022/0303 (COD) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). < 1_1_197605_prop_dir_ai_en.pdf (europa.eu) (12 October 2022).

Report from the Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technology' (European Commission 2019) [14].

Treaty on European Union, the Treaty on the Functioning of the European Union was adopted in Lisbon by 27 member states in 2007 and entered into force in 2009