UNIVERSITY OF KWAZULU-NATAL
SCHOOL OF LAW
HOWARD COLLEGE

A Comparative Analysis of the need for *sui generis* Artificial Intelligence Legislation in Kenya and South Africa

Report to funder: The Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University

Report authored by: Dane Bottomley
Principal investigators:
Professor Donrich Thaldar & Dr Paul Ogendi

February 2024

Strathmore University
Centre for Intellectual Property and Information Technology Law

Table of Contents

About this Report: The Road Forward

The purpose of this report is to provide the funder, the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, with an integrated report of the Kenyan and South African parts of our research. Full referencing to sources will be found in the respective country reports, which are attached hereto. The principal investigators' intention is that this report will form the basis for an academic article on the topic 'A comparative analysis of the need for *sui generis* artificial intelligence legislation in Kenya and South Africa' to be published in a peer-reviewed, open access journal. Once it is published, the principal investigators intend to disseminate the open access article as a white paper to policy-makers in both Kenya and South Africa. The funding received from the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, will of course be acknowledged in such an article. Given that this report will form the basis for the article, it is essential that this report is not disseminated publicly, as to avoid compromising the novelty of the intended article.

Acknowledgements

The South African part of this report is based on a 2023 LLM dissertation by Theshaya Naidoo – 'Analysing the need for *sui generis* AI legislation in South Africa in the face of international legal developments' – University of KwaZulu-Natal, under the supervision of the principal investigators. The Kenyan part of this report is based on research conducted by Meresa Atieno and Fidelice Opany under guidance of Dr Paul Ogendi. This present report was supported in part by draft versions generated with the help of OpenAI's ChatGPT, which were subsequently revised and expanded by the author; ChatGPT was finally also used to improve language and readability.

Acronyms & Abbreviations

AI	Artificial Intelligence
EU	European Union
Fintech	Technology used to support banking and finance
ICT	Information and Communications Technology
NHS	National Health Service
NIIMS	National Integrated Identity Management System
SMS	Short Message Service
UNESCO	United Nations Educational, Scientific and Cultural Organization

Glossary

Algorithm – Instructions or rules to be followed by a computer during problem-solving or data-processing.

Biometric Systems – Technology that uses body measurements or physical characteristics to identify individuals.

Blockchain – A peer-to-peer computer network that keeps a record of transactions.

Chatbot – A computer application designed to simulate human text or speech during a conversation with a user, typically with the intention of providing answers to user queries.

Cyberattack – The unauthorised access of a computer system or network with the intention of compromising the integrity of the system or network.

Cyberterrorism – The intentional use of computer networks and the internet to cause serious harm.

Deepfakes – Sophisticated AI-generated clones that realistically mimic the appearance and actions of real people.

Training Data – A very large amount of data used to train an AI model which the model then uses to create and define the rules by which it operates.

Abstract

The widespread adoption of artificial intelligence (AI) across various industries has led to a significant increase in its popularity in recent years. This growth is largely attributed to AI's ability to operate autonomously, generate insights independently from data, and continuously improve through learning processes. However, these very capabilities have raised concerns regarding potential errors, biases, and the risk of malicious use.

As a result, the need for precise and transparent regulation of AI development and use has become a critical and urgent matter. Despite its widespread application, there is a notable lack of specific regulation in countries like Kenya and South Africa. While existing laws might be interpreted to cover aspects of AI, there is still a need for a thorough evaluation of whether dedicated, AI-specific (*sui generis*) legislation is required.

This paper aims to analyse the current policies in Kenya and South Africa that are relevant to AI regulation. The objective is to determine the sufficiency of these policies and to explore the necessity and potential structure of *sui generis* AI legislation within the Kenyan and South African contexts.

The analysis indicates that while current legal frameworks in these countries do affect AI, they tend to be inconsistent and overlapping. In order to evaluate the effectiveness of existing regulations, we will compare them with regulations from various international jurisdictions. The conclusions of this paper will synthesise insights from the literature review and incorporate international best practices into the proposed regulatory frameworks for AI in Kenya and South Africa.

Introduction

AI has become a central aspect of modern policy and legal debates. Its gradual development and permeation into broader society has been spurred by its undeniable utility. Despite its recent increase in popularity, AI as a field of research has existed since as early as 1956. Despite this history failing to provide a universal definition of AI – thereby hindering research prospects – it is generally agreed that AI generally refers to hardware or software technologies that make machines autonomous from human beings.

AI reserves several apparent benefits over human agents: enormous computational ability; the lesser commission of errors; faster decision-making; round-the-clock availability; and the ability to undertake mundane, repetitive tasks. Sectors such as agriculture, healthcare, education and fintech are increasingly adopting AI initiatives.

Concerningly, AI can introduce considerable challenges to current legal, policy, social, economic, and political norms. Further, the autonomous decision-making capabilities of AI can have negative consequences due to potential errors, bias, and malicious intent. Accordingly, there is extensive debate on whether and how AI should be regulated to mitigate its adverse effects whilst fostering its benefits. This has led many to believe that implementing transparent and precise regulations governing AI development and application has become necessary and urgent.

Interestingly, some of the loudest calls for regulation have come from prominent stakeholders in the AI industry, such as Elon Musk, Bill Gates, Steve Wozniak and the late Stephen Hawking. The European Union's recent harmonised rules on AI (AI Act) has been heavily scrutinised by those favouring limiting regulation in favour of innovation, particularly the French, German and Italian governments. Similar hesitancy has been present in the United Kingdom and the United States' approaches.

An important impediment to regulation exists in the AI systems themselves. As already mentioned, there is still no universal definition of AI. Further, AI's complicated and rapidly evolving nature make it difficult for regulators to keep up with the technology.

These challenges to traditional *hard* regulatory frameworks have prompted the adoption of self-regulation or *soft law* by industry, governments, and bodies to govern AI applications. Although flexible enough for a developing sector, soft law methodologies lack direct enforceability. An alternative approach has been the utilisation of existing laws to bolster developing AI policies and strategies. The relevant regulation will depend on the legal and factual setting in which the technology is deployed.

AI development is still controlled by a few countries based outside of Africa, leaving those in developing nations to play catch-up, a considerable task when considering the progress made in the sector daily. Consequently, developing countries are significantly disadvantaged in how they choose to regulate this technology as they have to rely on models made for other countries and contexts.

National AI strategies are being taken advantage of to better link development and regulation. Smaller countries such as Mauritius, Rwanda, Senegal, and Benin are leading the African continent in this regard. Both Kenya and South Africa lack national AI strategies; however, both countries do have a plethora of applicable laws and regulations. These include the Kenyan Computer Misuse and Cyber Crimes Act, Consumer Protection Act and Data Protection Act, as well as the South African Protection of Personal Information Act and Patent Act.

There is no comprehensive analysis of whether and to what extent the extant policies are capable of regulating AI which could inform a debate on the enactment of *sui generis* AI legislation. This research seeks to propose recommendations for a tailored legal framework, including the exploration of *sui generis* AI legislation, if necessary, which addresses the legal challenges introduced by AI and ensures the protection of individual rights, societal well-being, and the promotion of innovation in this rapidly evolving technological landscape.

Accordingly, this paper will first consider AI through its uses in different sectors and the ethical, social, political and legal challenges it raises in Part A. In Part B, we will set out the current applicable statutes and regulations which apply to AI use in Kenya and South Africa, assessing their viability for future regulation. In Part C, we canvas key international developments in AI regulation, considering how they may be integrated to the Kenyan and South African contexts. In Part D, we consider a proposed AI regulatory framework for Kenya and South Africa. In Part E, we present key findings and provide recommendations based on the analysis of the previous sections before concluding.

Part A: Artificial Intelligence Uses and Challenges

Utilisation of Artificial Intelligence

AI is already being leveraged in a number of sectors to meet development goals and establish innovative solutions to regional problems.

Agriculture

Agriculture constitutes at least 33% of Kenya's GDP. However, inefficient supply chains, inadequate post-harvest services, and limited use of agricultural technologies restrict the sector's potential. Government has been relatively quiet on how it intends to promote innovation in agriculture. Nevertheless, some AI projects have already launched in this sector to assist farmers.

The ThirdEye project empowers farmers to use flying drones to monitor water, fertilisers and seeds, allowing them to optimise their yields. Eska uses satellite imagery to analyse crop photos, allowing farmers further information on weather patterns. Arifu uses AI chatbots over Whatsapp, Facebook Messenger and SMS to inform farmers on fertilisers appropriate for their soils.

These technologies increase the efficiency and accuracy of farmers' decisions, further helping to streamline supply chains and therefore bolster food security.

Healthcare

By offering enhanced accuracy in medical analyses, AI reduces the likelihood of human error, allowing for more precise medication prescriptions, thus minimising side effects. Its capabilities extend to making informed treatment decisions and recommending suitable medications. During pandemics, AI's role is pivotal in tracking patients, which is crucial for controlling disease spread.

In Kenya, the integration of AI in healthcare is still in its early stages. A notable example is AfyaRekod, an AI system that gathers real-time patient health data, facilitating faster medical response. Tambua Health, another innovative application, employs machine learning algorithms to detect and manage cardiopulmonary diseases. Additionally, Sophie Bot, a chatbot, offers valuable insights into reproductive health, making information more accessible to users. These developments begin a transformative journey in Kenya's healthcare sector through AI technology.

Fintech

The digital lending landscape in Kenya is experiencing rapid growth, with companies like Ceres Tech Limited and Letshego Limited at the forefront. These firms leverage AI to make informed credit decisions. AI algorithms analyse various data points, such as an applicant's savings history and repayment patterns, to evaluate their creditworthiness and determine the most appropriate loan type. This technology-driven approach streamlines lending, offering immediate credit approval without collateral. This efficiency sets digital lending apart from traditional financial institutions, like banks and microfinance entities, which often involve more time-consuming and resource-intensive procedures. Farm Drive specifically caters to small-scale farmers, using AI to assess credit eligibility based on land size, crop volume, and geographic location. Such innovations highlight the transformative role of AI in Kenya's Fintech sector, offering more personalised and accessible financial solutions.

Security and Surveillance

While regionalisation and globalisation can yield substantial economic and political gains, they also render national borders more vulnerable to insecurity and human trafficking. In response, AI can be a pivotal tool in bolstering national security. Biometric identification systems, a sophisticated application of AI, authenticate individuals based on unique physical or behavioural characteristics. Hard biometric systems utilise innate features like fingerprints, facial and voice recognition, and retinal patterns. Soft biometrics, conversely, analyse traits such as walking style.

Automated Border Control Gates, employing advanced convolutional neural networks, streamline the identification process at points of entry like airports. These systems enable swift and efficient traveller verification. Similarly, automated passport systems enhance the monitoring and inspection of passports at international borders, significantly increasing accuracy in individual identification, expediting decision-making, and conserving resources that would otherwise be allocated to manual security checks.

Beyond national security, AI also finds applications in more localised surveillance efforts. For instance, Missing Child Kenya, a non-profit organisation, harnesses AI to locate, trace, and reunite lost children with their families. Using Generative Adversarial Networks, this technology performs tasks like forensic imaging, photographic manipulation, and facial reconstruction to help search efforts. As of 2020, Missing Child

Kenya has been involved in over 780 search cases, demonstrating the impactful role of AI in addressing critical social issues.

Education

In education, the transformative potential of Artificial Intelligence (AI) is being harnessed to deliver personalised learning experiences. A prime example is Angaza Elimu, a UNICEF flagship project. This eLearning platform uses AI to provide students with customised notes and assignments tailored to their learning needs. Furthermore, it enables educators to evaluate student performance and offer resources aligning with each student's requirements.

Another innovative application is M-Shule, an SMS-based platform that employs AI to monitor student progress. By analysing this data, M-Shule delivers educational materials congruent with each student's learning objectives and pace, ensuring a more targeted and effective educational approach.

However, like other countries, the integration of AI in various sectors, including education, introduces many ethical, social, political, and legal challenges. These challenges often test the boundaries of existing regulations and require a nuanced understanding and approach. The following section provides an in-depth examination of these unique challenges posed by AI, highlighting the need for comprehensive and adaptive regulatory frameworks.

Ethical, Social, Political, and Legal Challenges of Artificial Intelligence

As with any technological revolution, the advent of AI raises important questions about its potential drawbacks and how to address them. Despite its numerous advantages and applications, there is growing concern in contemporary literature about AI's implications. Key issues include the risk of bias and discrimination, lack of transparency in decision-making, accountability gaps, and the potential infringement on fundamental rights and freedoms. This section delves into the ethical, social, political, and legal challenges AI presents.

Transparency and Explainability

The challenge of AI's 'black box' problem, where its decision-making process is opaque to users, raises significant concerns about transparency and explainability. While AI systems don't operate autonomously and require human involvement in defining problems, modelling, algorithm design, and data manipulation, the internal workings often remain hidden. This lack of visibility into the AI's decision-making process makes it difficult for humans to understand why a specific output or decision was made.

The consequences of this opacity can be profound, as noted by Desai and Kroll, who highlight instances where individuals have faced adverse decisions without clear understanding due to the software's inscrutability. In healthcare, this opacity can affect informed patient consent.

Explainability is vital for both developers and users. For developers, it aids in debugging and refining the AI, while for users, it builds trust and enables informed responses, including legal recourse if necessary. Research in explainable AI focuses on making AI systems more interpretable and understandable. This includes local explanations, which detail decision-making in specific instances, and global explanations, which consider the AI's overall behaviour. Other strategies for enhancing transparency include disclosing AI's role in decision-making and its limitations. Despite ongoing efforts, fully explainable and transparent AI has not yet been achieved.

Discrimination, Bias, and Unfairness

While capable of outperforming humans in speed and computational ability, AI is not immune to flaws such as discrimination, bias, and unfairness. Bias in AI can manifest in various forms: algorithmic bias due to flawed decision-making algorithms, sample bias from inadequate or excessive training data, and prejudice bias, which stems from incorrect societal assumptions embedded in the data, like presuming most doctors are male.

The EU Agency for Fundamental Rights warns of the risks of algorithmic discrimination, especially in automated decision-making processes in public and private sectors, affecting areas like job selection, credit assessment, and legal judgments. ProPublica found that a US algorithm used in bail and sentencing favoured prejudice against black defendants, while other algorithms have shown bias in mortgage rates and job recruitment.

In Africa, the challenge is amplified due to reliance on imported technologies and underdeveloped data infrastructures. AI systems often use Western datasets, leading to inaccuracies in recognising African patterns and languages, and a lack of support for diverse African languages exacerbates the issue. For example, Microsoft Bing only offers machine translation for Swahili and Afrikaans, unlike DeepL's coverage of numerous European languages. This technological gap hinders Africa's integration into the global digital economy. Suggestions to mitigate AI bias and discrimination include open algorithms, a human-in-the- loop approach, and certification systems. However, these are not perfect solutions. Human involvement isn't always ideal, particularly where human error could have severe consequences. Moreover, making algorithms transparent doesn't necessarily mean their logic will be universally understood.

Accountability and Responsibility

Algorithms are increasingly central in decision-making across both private and public sectors. This decision-making can be fully automated, with AI-driven decisions implemented directly or mixed, involving human oversight or review. However, AI presents accountability challenges due to its opacity. Even when AI delivers a definitive conclusion, like denying credit, the process behind this decision, especially with complex algorithms like deep learning and neural networks, is often not transparent.

This lack of transparency is exacerbated by the proprietary nature of algorithms, typically developed by private companies and possibly sold to public authorities. The secretive nature of these algorithms, protected as trade secrets or intellectual property, hinders scrutiny and understanding by affected parties. This secrecy makes it challenging to determine the basis for liability in AI-implemented decisions.

Moreover, current liability rules are designed around human actions, not AI. Despite AI's potential for serious errors, they lack legal personhood and thus cannot be held accountable. This leads to critical questions: Should humans be liable for AI's unforeseen errors? Who compensates for damages caused by AI? Should laws in areas like contracts and torts be adapted for AI contexts?

The situation is complicated when technical AI decisions are interpreted and implemented by non-technical personnel, often leading to misunderstandings. The AI life cycle involves numerous parties – designers, developers, suppliers, deployers, and users – making it difficult to pinpoint responsibility for AI errors. This creates a 'many hands problem', where no single entity in the decision-making chain is accountable for AI's negative consequences, leading to potential 'suboptimal equilibria'. Additionally, the 'many eyes problem' arises from different AI systems using varied decision criteria, further complicating accountability. Addressing these 'many hands' and 'many eyes' issues is crucial to prevent accountability gaps, where no one is held responsible for AI's errors or omissions, and to avoid accountability surpluses, where procedures are inefficiently layered.

Threat to Political and Social Stability

Historical records are filled with examples of manipulated photos, videos, and information, often used to create misleading or disparaging narratives about political figures. This practice dates back centuries, with altered images of figures like Marie Antoinette and Louis XVI.

The advent of technologies like cameras further enhanced the potential for information manipulation, a trend that has intensified in the AI era, particularly with the rise of deepfakes.

Deepfakes are created using software that emulates human brain neurons. This technology allows manipulation of a person's facial expressions in videos, achieving highly realistic results.

While deepfakes have benign uses, such as entertainment and advertising, they pose significant risks. They can damage reputations, distort public opinion, and even affect international relations, especially in politically fragile environments. The 2007/08 post-election violence in Kenya, exacerbated by misinformation via SMS, exemplifies the potential for technology-facilitated misinformation to incite conflict.

Regulating AI tools like deepfakes is crucial, but overregulation risks stifling innovation and legitimate uses. Legal exemptions may balance innovation and human rights, yet they can also enable harmful AI applications. A notable legal case is Gonzales v Google 21-1333, where the Gonzalez family sued Google, alleging that its AI algorithms facilitated Islamic State recruitment on YouTube, leading to Nohemi Gonzales's death in the 2015 Paris attacks. The US trial court must decide if internet companies are liable for content targeted by their algorithms under Section 230 (1) (c) of the US Communications Decency Act of 1996.

The challenges posed by deepfakes and the Gonzales case highlight the need for a delicate balance in AI regulation within the political sphere, weighing the freedom of expression against the rights of third parties.

Security and Surveillance

The application of AI in security and surveillance offers benefits like time and resource efficiency, enhanced data sharing between authorities, and more accurate decision-making. However, these advantages come with significant risks. First, AI technologies may inadvertently perpetuate racial, ethnic, or religious biases. An example is South Africa's border control, where AI usage has led to discrimination and stereotyping. Second, biometric identification systems, while efficient, can pose challenges for refugees and asylum seekers who may lack the extensive documentation required for biometric verification.

The lack of a robust legislative and regulatory framework for AI in security and surveillance heightens the risk of misuse.

The Kenyan government's Huduma Namba initiative, introduced in 2019 under the National Integrated Identity Management System (NIIMS), aimed to enhance national security by collecting, processing, and analysing biometric and location data. This initiative, intended to identify security threats and improve response capabilities, was halted by the High Court due to the absence of legislation ensuring biometric data protection. Such data could be exploited for political surveillance and oppression without proper safeguards. Studies, including one by Feldstein, show that AI is increasingly being adopted for political surveillance, particularly in authoritarian regimes and countries with low levels of political rights.

Privacy and Data Protection

Data, particularly personal data, is fundamental to AI development, necessitating a robust legal and policy framework to regulate its access and usage. A case in point is the 2016 partnership between Google and the Royal Free London NHS Foundation Trust, utilising DeepMind's technology for acute kidney injury management. This initiative faced criticism for bypassing due process in data acquisition and not sufficiently addressing privacy concerns, with patients lacking control over their data, which was later transferred to the US.

The involvement of foreign AI developers often leaves data subjects with little control over their data, a concern amplified by the ongoing monetisation of data. Additionally, technologies like facial recognition algorithms and widespread CCTV deployment enable seamless identification and tracking, infringing on privacy rights and potentially facilitating oppressive surveillance, limiting freedoms of movement and expression.

A significant risk is data repurposing for unconsented uses, as highlighted in the NIIMS case. The Nubian community, for instance, feared that data collected ostensibly for security could be used for other purposes. Although Section 51 of the Data Protection Act permits data collection and processing by security agencies for national security or public interest, the broad interpretation of 'public interest' could lead to unauthorised usage. The NIIMS case also noted the lack of a robust framework to protect the integrity of collected data. Moreover, centralising data storage increases the risk of breaches and cyberattacks.

Given these substantial privacy and data protection concerns posed by AI, all parties involved in AI development must adhere strictly to data protection principles, safeguarding both the integrity of the data and the privacy rights of individuals.

Part B: Current AI-Related Legal Frameworks

Kenya

As described above, Kenya has no specific legislation governing AI. However, it has several existing laws and regulations which are relevant to the regulation of AI.

The Constitution of Kenya

The Kenyan Constitution includes provisions that significantly influence AI. Article 10 highlights national values like equity, social justice, and transparency, mandating their adherence to AI applications. This requires public and private entities to use AI to ensure non- discriminatory and transparent decision-making processes.

Furthermore, Articles 11(2) and 40(5) advocate for protecting Kenyan intellectual property rights, directing AI developers to comply with these laws. Article 27 prohibits bias and discrimination practices that AI can exhibit. Also, Article 31 emphasises the right to privacy, limiting AI usage that infringes on personal data.

Additionally, AI in surveillance and security must not violate freedoms like the right to movement (Article 33). Article 46, which ensures consumer rights, implies that AI technologies must be high-quality and safe. These constitutional provisions provide a robust framework for AI regulation in Kenya.

The Data Protection Act, 2019

AI relies heavily on data, both private and public. The Data Protection Act (DPA) of Kenya governs this data's handling, usage, and protection. It defines 'data controllers' as those who determine data processing purposes and means and 'data processors' as entities processing data on behalf of the controller. This encompasses various roles within the AI development process.

Fundamental principles outlined in Section 25 of the DPA for AI developers include the limitation of purpose (restricting data use to its original intent), data accuracy (ensuring data is current and correct to minimise bias), lawful and transparent processing, and storage limitation (not retaining data longer than necessary). Non-compliance provides grounds for legal claims under the Act.

Given AI's potential risks to personal data, the DPA mandates a data protection impact assessment under Article 31, requiring high-standard data management and breach prevention. Article 35 restricts decisions made solely by automated processing, including profiling, if they have legal effects on individuals, advocating for human oversight in AI decision-making. The 2021 Data Protection Regulations reinforce this by requiring data processors to inform subjects about automated processing.

The Act also emphasises obtaining prior consent from data subjects, limiting AI developers' ability to process or commercialise data harmfully. Additionally, it restricts the transfer of data outside Kenya, supported by Section 4, which extends the DPA's jurisdiction extraterritorially.

Computer Misuse and Cyber Crimes Act of Kenya, 2018

While AI can bolster security domestically and internationally, it also poses risks of cyberattacks threatening national security systems. The Computer Misuse and Cyber Crimes Act in Kenya aims to prevent such misuse by facilitating the detection, investigation, and punishment of cybercrimes. It criminalises unauthorised access to computer systems, data interference, cyberterrorism, and false data publication, making AI operators responsible for preventing their systems from being used for these illegal acts.

But despite its widespread use, Kenya faces legal gaps in regulating AI, particularly in managing facial recognition technology. The absence of regular impact assessments raises concerns over adherence to privacy rights. While the Security Laws (Amendment) Act of 2014 supports using digital tools by security agencies for threat detection and elimination, there is a lack of legislative safeguards to prevent the misuse of these tools in violating civil rights, including freedom of movement and expression.

Kenya Information and Communications Act, 1998

This legislation governs the ICT sector, electronic commerce, and telecommunications services, affecting AI developers and deployers within these industries. Key provisions include Section 29 which bans the misuse of regulated systems, and Section 31 which forbids the interception and disclosure of messages. Consequently, this Act mandates high standards in the development and use of AI technologies by all involved in the AI lifecycle.

Consumer Protection Act No. 46 of 2012

The Consumer Protection Act in Kenya, aimed at enhancing consumer welfare, implicitly addresses the risks associated with AI, whether used as standalone products or as components in other products. The Act promotes fair, ethical practices and prohibits misrepresentation of product standards, indirectly curbing the use of faulty AI systems that could harm health, body, or property.

It empowers consumers to initiate legal action for rights violations, addressing potential risks AI systems pose. Additionally, it entitles consumers to information about the quality and standards of products and services. While the Act doesn't explicitly mention AI, it requires AI developers, suppliers, and deployers to disclose and mitigate quality risks associated with AI systems.

However, the Act lacks clarity on who bears responsibility for AI-related breaches, presenting challenges due to the numerous stakeholders in AI's lifecycle.

The Health Act No. 21 of 2017

The Health Act is a crucial legislation governing AI in healthcare in Kenya. Its primary objectives include regulating healthcare services, products, and technologies. Of relevance is Part VII, which focuses on the regulation of health products and technologies, encompassing AI-integrated solutions.

This Act establishes a regulatory authority responsible for licensing health products and technologies, inspecting their manufacturing and storage, and conducting post-market surveillance. AI-based health technologies are subject to these regulations and can only enter the market after meeting the criteria set by this authority. This mirrors the proactive regulation approach seen in the EU Act for high-risk AI systems in healthcare.

Additionally, the Act forms the Kenya Health Professions Oversight Authority, tasked with addressing patient complaints, further ensuring the responsible deployment of AI in healthcare.

Intellectual Property Laws

The use of AI in inventions raises questions about AI's role as an inventor. In significant jurisdictions like the US, UK, and EU, only humans can be listed as patent applicants and own patents. While Kenyan law hasn't explicitly addressed this, it is likely to align with this view. The Kenyan Industrial Property Act defines an inventor as someone who devises an invention, implying that AI, lacking legal personhood, cannot hold patents.

AI's impact is significant in copyright law, especially with models like ChatGPT creating copyrightable content. The Kenyan Copyright Act of 2001 defines an author as a natural person, excluding AI from ownership. It is unclear whether humans can claim full or joint authorship with AI. Additionally, AI systems, like ChatGPT, are trained on vast datasets, including copyrighted materials, raising questions about text and data mining. While the Act allows fair dealing for scientific research, it does not clearly define 'fair dealing' or the scope of permissible research, leaving legal uncertainties around AI’s data usage.

The case of Communications Commission of Kenya & 5 others v Royal Media Services Limited & 5 others (2014) indicates a move towards a ‘fair use’ approach but lacks clarity on AI’s legal boundaries in text and data mining. The existing Intellectual Property Bill does not significantly update this framework, leaving gaps in adapting to technological advancements.

Apart from the preceding legislation, Kenya has also put in place policies which may impact AI.

Digital Economy Blueprint

The 2019 Digital Economy Blueprint broadly defines the digital economy, including AI, as sectors using digital communications and technologies like the internet and mobile networks. It identifies AI as a catalyst for Kenya’s transition from a lower-middle-income economy to an emerging or advanced economy. The Blueprint outlines five pillars to drive this digital transformation: digital government, digital business, infrastructure, innovation-driven entrepreneurship, and digital skills and values.

ICT Ministry Strategic Plan 2023-2027

This Strategic Plan acknowledges the efficiency and productivity gains from new technologies like AI, blockchain, and others. It explicitly includes AI in Key Result Area 7, focusing on cybersecurity, data management, and emerging technologies. Strategic Objective 13 aims to foster a secure digital ecosystem, with the adoption of emerging technologies like AI as a critical outcome indicator. The Plan also emphasises educating citizens about data protection and developing AI skills to address skill gaps.

Key recommendations include:

1. Amending laws related to security and surveillance to regulate digital tools, like facial recognition, ensuring due process and protection of fundamental rights.
2. Updating the Copyright Act to clarify copyright eligibility for AI-generated works and to adapt text and data mining exemptions for technological advances. The 2020 Intellectual Property Bill should be revised to reflect AI’s impact on intellectual property.
3. Developing a national AI Strategy to promote innovation.

4. Conduct regular sector-specific assessments to evaluate AI's impact and determine the need for specific legislation.
5. Issuing soft laws, such as guidelines on ethical AI, to provide predictability, even if they are not legally binding.

South Africa

Protection of Personal Information Act (POPIA)

AI has clear benefits in recruitment and cost savings, but many academics raise concerns about its risks to privacy and equality. Business leaders stress the importance of privacy for ethical AI, which involves respecting user privacy, securing data, and ensuring protection. This right, protected under section 14 of the Constitution, allows individuals to control their public disclosures. Section 36 recognises that privacy may be limited for other rights like information access. Addressing fairness is crucial to balance large data organisations' power and individuals' power. Policymakers play a key role in regulating AI, ensuring fair and accurate data handling.

AI's challenge in processing personal data lies in ensuring fairness. The GDPR and South Africa's Protection of Personal Information Act (POPIA) safeguard privacy while allowing information access and expression. POPIA defines personal information broadly, including opinions and online identifiers. The Act balances individual privacy with societal needs, such as security and workplace efficiency. It requires informed consent for processing personal data, except under general authorisations.

Section 71 of POPIA addresses AI in decision-making, preventing biased or inaccurate outcomes that can affect socio-economic factors, like credit or employment opportunities. Accurate data handling can minimise biases. POPIA demands transparency in data collection purposes, allowing individuals to make informed choices about their data.

POPIA applies only to processing personal data, excluding de-identified data from its scope. AI developers must comply with POPIA, ensuring lawful and transparent processing with robust security measures. However, fears persist about AI's potential to surpass human intelligence, the so-called 'singularity', highlighting the need for ongoing research and transparent communication about AI risks.

POPIA’s data minimisation requirement presents a challenge, as AI requires large datasets for effective training. This increases privacy and security risks, balancing against the need for extensive data for AI performance. The Act provides a foundation for ethical AI use in South Africa, emphasising transparency and informed consent. It also highlights the importance of data security but acknowledges the constraint data minimisation poses on AI model training. The Act’s adaptation to include ‘data anonymisation’ could help resolve this issue, allowing for the use of de-identified data in compliance with its principles.

Consumer Protection Act, 68 of 2008

The Consumer Protection Act (CPA) in South Africa governs the sale of goods and services, including AI technologies. It aims to foster an equitable economic environment, protecting societal values. Under the CPA, AI systems providing goods or services fall under the Act’s purview due to their tangibility in integrated systems. Section 22 mandates that suppliers offer clear, understandable information to consumers, which is crucial for AI-driven services, ensuring informed decisions and addressing potential biases.

Section 41 assesses the quality and performance of AI-driven products, emphasising accuracy and effectiveness. The Act imposes strict liability for product defects, holding all supply-chain parties accountable. Consumers can claim remedies for AI products’ issues, but the evolving nature of AI algorithms complicates evaluating performance against initial promises.

AI’s ‘black box’ nature makes identifying failures or defects challenging. Consumers don’t need to prove supplier negligence under section 61 but must establish the existence and causation of a defect or hazard. The technical complexity of AI systems complicates this process, requiring expertise beyond the average consumer’s reach.

AI’s data processing risks include potential misuse or exploitation of consumer data. Section 68 requires careful data management by AI systems, yet it doesn’t fully address challenges like machine learning or the transparency of large-scale data processing. The reliance on data from multiple sources, including third parties, challenges suppliers’ control and visibility over data processing, necessitating robust safeguards and data integrity and transparency monitoring.

Section 61 allows claims for damages from defective AI systems, while section 41 offers consumers refunds or compensation for poor AI product performance. However, due to technical complexity, consumers may struggle to identify or prove faults in AI technologies.

The CPA provides a framework for transparency, accountability, and consumer remedies in AI applications, but its integration with AI has limitations. Consumers' technical knowledge gaps hinder effective remedy seeking, and the Act lacks specific guidelines for AI-related issues.

Incorporating detailed AI guidelines in the CPA, including technical expertise for causation and mandating disclosure of AI algorithms, could enhance transparency and ease bias detection, making the Act more effective for AI technologies.

South African Patents Act

South Africa became the first country to grant a patent to an AI system, DABUS, for inventing a device and a food container. However, this decision faced criticism as the South African Patents Act, under Section 25(1), requires inventions to be new, involve an inventive step, and be useful, with applications traditionally limited to natural persons. The Act's language suggests inventors must be human, not AI like DABUS.

Critics argue that AI cannot legally be an inventor, highlighting a gap in South African patent law, which currently only performs a formal examination of patent applications. This gap allowed DABUS's patent, contrasting with more rigorous systems like the European Patent Office that rejected it. Proponents, like Thaldar and Naidoo, interpret this acceptance as aligning with South Africa's policy to promote innovation in the fourth industrial revolution era. However, this approach could lead to patents lacking human creativity, potentially stifling innovation.

The Patents Act's Section 28 addresses computer programs, stating they are not inventions unless producing a new technical result. This provision allows for patenting AI algorithms that yield tangible outcomes but does not fully clarify the patentability of AI-generated inventions. The Act's lack of substantive examination during the patent process means it doesn't effectively address the complexities of AI inventions.

The broader context involves balancing promoting innovation with safeguarding human creativity and innovation, the foundations of patent law. Extending personhood to AI, as some suggest, overlooks human unique moral and ethical capacities and could complicate legal and societal frameworks. While allowing DABUS's patent, the Act does not clearly define AI's role in inventions, leaving open questions about AI's place in the patent system and the need for more robust examination processes.

Medicines and Related Substances Act (MRSA)

In South Africa, unequal access to healthcare and a shortage of healthcare workers highlight the potential benefits of AI in prediction, prevention, diagnosis, and treatment. However, legal, ethical, and practical challenges impede AI implementation in healthcare. Donnelly identified three legal barriers: the registration process for new AI health technologies, ethical framework considerations, and liability regulation for harm caused by these technologies.

The Medicines and Related Substances Act (MRSA), which governs the registration of drugs and medical devices, includes a broad definition of medical devices that could encompass AI technologies. However, general software not meeting this definition in healthcare applications falls outside the MRSA's scope, leading to ambiguities in AI classification.

The Act's underdevelopment is acknowledged, with recommendations to draw from international frameworks like the International Coalition of Medicines Regulatory Authorities (ICMRA) and the EU's Artificial Intelligence Act (AIA). This gap is particularly evident in the South African Health Products Regulatory Authority (SAHPRA) not yet registering AI medical devices, suggesting the need for an AI-specific regulatory framework.

AI's functionality in healthcare, based on vast datasets, faces the challenge of bias, especially when designed in first-world countries. Integrating healthcare process platforms and diverse, representative training datasets is essential for accurate, unbiased medical decisions. This approach aligns with the Protection of Personal Information Act (POPIA), mandating patient consent for data use.

The dynamic nature of AI technologies requires re-evaluating the regulatory review model for medical devices, accounting for AI's evolving nature. Questions of AI autonomy, interaction, reliability, and implementation need addressing in regulation.

South African healthcare has begun incorporating AI, like automated dispensing machines regulated by SAPC's Good Pharmacy Practice Standards. However, a comprehensive regulatory strategy focused on AI and machine learning software, covering development to operational stages, is needed.

To effectively regulate AI in healthcare, the MRSA's provisions should be aligned with international standards like the EU's AIA, ensuring a comprehensive and globally consistent approach to evaluating, monitoring, and regulating AI medical devices. This approach, supported by Townsend, emphasises the need for inclusive and adaptable regulatory definitions to address the unique challenges of AI in healthcare.

Electronic Communications and Transactions Act (ECTA)

The autonomous nature of AI has revolutionised the invention process, yet South Africa's regulatory framework doesn't fully account for AI-created material. The Electronic Communications and Transactions Act (ECTA) regulates automated electronic transactions, including those involving AI, but lacks clarity on contracts autonomously amended by AI.

Section 20 of the ECTA covers electronic contracts facilitated by AI, creating legal uncertainty in cases where AI unilaterally modifies contract terms. This raises questions about the legal obligation of parties represented by AI and the potential for evading contractual responsibilities through claims of mistake or lack of authority.

AI's ability to independently conclude contracts reshapes commercial transactions. The ECTA recognises the legal validity of contracts formed by AI, with Section 20(c) establishing that parties are presumed bound by the contract, even without direct review. POPIA's Section 71(2)(a)(ii) also recognises the legality of automated contracts, provided appropriate measures protect the involved parties.

Section 25(c) of the ECTA assigns liability for automated transactions to the AI programmer or the person who commissioned the AI. This liability may be mitigated if the AI deviates from its programming. However, the Act acknowledges that software products may have errors, which can be addressed through updates.

While Sections 20 and 25 of the ECTA recognise AI's role in transactions, establishing contractual validity and liability, they don't fully address the potential for AI to evade contractual responsibilities. This gap creates ambiguity and potential exploitation in AI-formed contracts. Therefore, the Act needs amendments to ensure fairness, transparency, and clear accountability in AI-involved contracts.

Part C: International Best Practices for AI Legislation

Global Trends in AI Regulation

The potential for AI to greatly benefit society but also cause great harm is an important consideration in any regulatory debate. Accordingly, stringent, responsible, and ethical regulations are essential. The corresponding fear of overregulation of AI, however, may lead to a lack of robust rules in the interests of innovation. Nevertheless, the vast impact of AI has inspired calls for regulation among governments, industries and academics. History suggests that a laissez-faire approach to disruptive technologies is ineffective. Therefore, the key consideration is how to regulate this new technology effectively. Global regulatory trends are diverse. This section will analyse key regulatory models for AI as they have been explored in other jurisdictions.

Risk-Based Approach

A risk-based approach to AI regulation identifies and mitigates AI-associated risks, assessing AI systems' potential dangers to formulate appropriate regulations. The EU AI Act utilises this approach, categorising AI risks into a four-tier framework, targeting significant threats to fundamental rights and safety. However, critics have argued that this approach often masks political decision-making under regulatory guise.

In contrast, the prescriptive approach sets explicit standards for AI systems, limiting entities' flexibility in compliance methods. This approach overlooks political enforceability challenges and contrasts with applied ethical strategies. The EU's Artificial Intelligence Act embodies a risk-based method with stringent requirements for high-risk AI systems, while the UK favours principles that encourage safe, innovative AI use. China adopts a hybrid approach, combining prescriptive, rights-based, and risk-based elements, and categorises AI risks more extensively than the EU and the US.

Academics highlight the EU's 'umbrella approach', which aims to boost global AI competitiveness and foster collaboration, especially between the US and China, proposing regulatory and ethical frameworks. They emphasise the role of ethics in AI governance, acknowledging that ethical considerations extend beyond legal compliance.

The unpredictability of AI systems presents technical challenges for accountability in governance. Dominant global players like the US, Europe, and China shape AI governance with national policies and laws, influencing global regulatory trends. The EU's model focuses on fundamental rights and ethics, while the US balances AI innovation with risk management, and China prioritises technological advancement for global leadership. Post-Brexit, the UK is developing its AI regulatory framework, potentially drawing lessons from the EU.

Globally, a consensus for a risk-based approach to AI regulation is emerging, as seen in the G7's International Guiding Principles on Artificial Intelligence. The EU AI Act categorises AI into prohibited, high-risk, and minimal-risk categories, each with specific requirements. This approach enhances AI system safety and security, enables efficient market entry, and provides sector-agnostic compliance.

However, defining AI for legislation is challenging, and overly broad definitions like the EU AI Act risk stifling innovation. Implementation uncertainties arise with evolving AI models. While offering predictability, such an approach may struggle to keep pace with rapid AI advancements. The EU AI Act coexists with other relevant laws like the GDPR, requiring significant resources and potentially leading to market concentration.

In summary, a risk-based approach offers safety and standardisation but faces challenges in definition, flexibility, and market impacts.

The European Union's AI Act, passed by the European Parliament on June 14, 2023, represents a pioneering effort in AI regulation. It safeguards EU values and principles, including transparency in generative AI tools and banning real-time facial recognition. This risk-based legislation categorises AI systems according to potential harm to human rights or interests, imposing varying restrictions.

Critics like Glauner argue the Act risks overregulation, potentially stifling AI development in critical areas like healthcare. This view aligns with Burri and Von Bothmer, highlighting that while the Act prohibits specific AI uses, it doesn't halt AI development in these areas. The rise of generative AI, with broad and unpredictable applications, challenges this restrictive framework.

The EU's AI strategy contrasts China's, emphasising ethical AI outcomes and fundamental rights protection. Initially adopting a soft law approach with the 2019 Ethics Guidelines for Trustworthy AI, the EU shifted towards legislative regulation with the draft AI Act. This framework categorises AI systems by risk levels, with varying regulatory requirements from minimal to absolute prohibition for extreme-risk applications.

Critics argue the EU's rigid and prescriptive measures may not be sustainable and could hinder a competitive AI market. Proponents, like Del Castillo, believe the Act promotes innovation. However, concerns about the Act's complexity and limited transparency remain, particularly in the context of machine learning algorithms.

The Act's extraterritorial impact could lead to a 'Brussels Effect,' influencing global AI standards. US technology investments in the EU may dilute the Act's effectiveness due to ethical and technical complexities. Academics debate the EU's potential as a global AI leader, with some suggesting limitations due to its lack of a leading AI industry and cohesive defence strategy.

In the UK, post-Brexit legislative initiatives focus on AI's societal impacts, adopting a non-statutory, principle-based approach. Considering AI's application context, the UK strategy emphasises a balanced, innovation-friendly framework.

Adapting the EU's approach to South Africa could align with its commitment to human rights and ethical considerations. However, implementing a comprehensive risk-based system in South Africa faces challenges due to resource limitations and data disparities, potentially hindering effective AI categorisation and regulation.

Smuha argues that the race to AI drives a parallel race to AI regulation. As AI risks become more apparent, regulators are urged to adopt a broader view, considering factors beyond the benefits of AI to ensure it is 'trustworthy.' AI's complexity and the ambiguous international legal context pose significant challenges, making regulation difficult but necessary to foster AI acceptance and legal certainty and improve countries' competitive standing in AI development.

A rights-based approach to AI regulation emphasises fundamental human rights, aiming to balance innovation with human rights preservation. This approach focuses on making individuals active participants in AI development, fostering accountability. However, it faces criticisms for its ambiguity and practical implementation challenges.

Sector-Specific Regulation

AI regulation can be achieved through hard and soft laws, targeting specific sectors prone to AI risks. This can be executed via a cross-sectoral approach establishing minimum safeguards across all industries and a sector-specific approach addressing particular risks, like the EU AI Act's revision of the Machinery Directive for industrial machinery.

The advantage of sector-based regulation lies in its ability to cater to unique sectoral needs, offering tailor-made regulations and flexibility to accommodate emerging AI types. It also allows for the gradual identification of legislative gaps and unregulated AI applications, laying a solid foundation for specialised legislation.

However, the effectiveness of this approach hinges on regulatory expertise. Agencies lacking in AI knowledge may struggle with effective oversight, and hiring experts incurs social costs. Additionally, sector-specific regulations risk lagging behind rapid technological advancements and may inhibit innovation.

Effective sector-based regulation also requires coordinated efforts among regulatory bodies. For instance, an AI medical device might raise issues spanning data protection and medical negligence, complicating the legal process for complainants. Diverse regulatory practices across agencies can lead to inconsistency and unpredictability. Moreover, sector-specific regulations may leave AI developers and importers uncertain about their obligations and compliance methods compared to a risk-based approach.

In the US, AI regulation is still in its early stages, marked by patchwork regulations at state levels addressing risks like bias, privacy, and security. This approach contrasts with the EU's comprehensive AI regulation. Federally, efforts encompass universal initiatives, sector-specific applications, and legislative proposals. The FDA, for example, regulates AI in medical devices. The US aims to balance public safety, transparency, and innovation with suggestions for a pragmatic, voluntary framework for AI regulation.

The US's initial steps in AI governance came with the Trump Administration's Executive Order, contrasting with the EU and China's approaches. Between 2019 and 2022, 27 AI laws were passed across 14 states, focusing on AI opportunities and threats. However, the federal framework has lagged behind the EU in developing a robust AI governance model. The White House Office of Science and Technology Policy established five principles for automated systems. Congress has introduced AI-related bills at state and local levels, like the Algorithmic Accountability Bill and the California Consumer Privacy Act.

The US's patchwork AI regulation, including the Algorithmic Accountability Act, relies heavily on self-regulation and lags behind China and the EU's more advanced regulations. The National AI Initiative Act of 2020, establishing the National Artificial Intelligence Initiative, prioritises AI research and application for economic prosperity and national security.

Academic opinions on US AI regulation are divided, with some favouring minimal regulation to foster innovation and others advocating for more aggressive regulations. Despite steps like the Government Accountability Office establishing an AI accountability framework, comprehensive federal legislation is lacking. Like section 230 of the Communications Decency Act, existing regulations don't fully address AI risks.

The US's initial AI development was military-focused, but its commercialisation necessitates a robust regulatory framework. The 2019 Executive Order EO 13859 introduced a federal risk- based approach to AI regulation, encouraging various risk reduction strategies. However, this guidance is not comprehensive.

Considering the fragmented US AI regulatory landscape, South Africa should aim for national consistency in its AI regulations, developing national principles based on values like fairness, transparency, accountability, and safety. This approach ensures AI development benefits all citizens and fosters trust, which is particularly important in a country with a history of inequality. Local flexibility may not be suitable in South Africa due to the challenges in developing effective, community-accommodating AI regulations.

China's evolving role in global AI governance, highlighted by Cheng and Zeng, is impacted by its geopolitical context. Its approach, which fosters innovation and shared prosperity, contrasts with the EU's emphasis on protecting fundamental rights and promoting ethical AI. Goyal notes China's efforts in developing a regulatory system and enhancing intellectual property protection, aiming to become a global AI innovation centre and hold AI accountable for potential harm.

China's AI strategy, supported by 23% of AI companies like Alibaba and Tencent, employs a top-down approach, setting broad goals and encouraging a bottom-up approach from businesses. Zeng suggests that China aspires to shift from norm-taker to norm-shaper in AI regulation, aiming to establish itself as a world AI innovation leader by 2030.

China's governance initiatives target uniform AI norms and standards, adopting controversial AI technologies like facial recognition and AI-augmented social governance. The Cyberspace Administration of China (CAC) manages generative AI services, requiring security assessments and implementing measures to ensure AI services align with socialist ideals. The China Academy of Information and Communications Technology (CAICT) assists in assessing AI systems, while laws like the Personal Information Protection Law (PIPL) and Cybersecurity Law (CSL) regulate data protection and privacy.

Challenges include balancing military and healthcare AI applications and managing the decentralised, often disjointed local AI strategies across provinces. This fragmented approach can lead to waste and exploitation. The Chinese government incentivises local AI strategies, but coordination issues remain.

China's comprehensive legislative framework, addressing data protection, privacy, and socio-economic issues, places regulators in a position to balance international competitiveness and market abuse prevention. The potential for a global regulatory impact counters the EU's potential to influence global AI regulation.

For South Africa, adopting China's model involves prioritising industries where AI can drive growth and competitiveness, like healthcare, agriculture, and manufacturing. Coordinated strategies leveraging local expertise and resources are crucial. Establishing regulatory bodies focused on AI safety and ethical frameworks, as China has done, will be integral to South Africa's AI regulatory framework.

In conclusion, the review of diverse AI regulatory approaches in various jurisdictions reveals key lessons in research, development, and early adoption. The US and EU emphasise these areas, essential for building the expertise to address AI-related issues effectively.

This chapter highlights the importance of adopting global best practices and adapting them to local contexts. As AI increasingly impacts different sectors worldwide, this comparative analysis offers insights for South Africa. It underscores the need to create a regulatory framework that aligns with global standards and respects South Africa's unique socio-economic landscape, balancing innovation with ethical and societal values. The following chapter will discuss alternatives to *sui generis* AI legislation tailored to South Africa's needs and conditions.

Regulatory Sandboxes

Regulatory sandboxes provide a controlled environment to test innovative technologies, proving successful globally since their inception by the UK Financial Conduct Authority in 2014. Adopted in around 40 jurisdictions, these sandboxes have inspired similar approaches in AI regulation in the UK and EU.

Key benefits of regulatory sandboxes include fostering public-private partnerships and enabling high-quality, sector-specific regulation that can be adapted across various industries. This model not only enhances competition and innovation but also ensures a tailored regulatory approach that respects each country's unique political, social, and legal contexts.

For instance, the EU AI Act’s sector-wide application is complemented by targeted regulations in specific areas like machinery. Similarly, the UK’s comprehensive AI assurance roadmap includes specific directives for industries like human resources. Crucially, these regulatory strategies aim to balance innovation with protecting fundamental rights and freedoms.

Part D: Proposal for a Kenyan and South African AI Regulatory Framework

The Necessity of *sui generis* AI Legislation

The Oxford English Dictionary defines '*sui generis*' as unique or of its kind. In legal terms, it refers to a law tailored to a specific entity or activity. In South Africa, integrating AI into existing legal frameworks like data protection and consumer rights is essential, but creating a *sui generis* AI regulatory framework may not be the most effective approach.

For AI regulation to be effective, it must be necessary, justifiable, adhere to the rule of law, be implemented fairly, involve public participation, be flexible, and mitigate AI risks. Currently, AI in Kenya and South Africa lack a specific legislative framework and are therefore treated as *sui generis* by default. Yet, there are existing laws which currently address some AI risks and could be amended to cover AI-specific issues more comprehensively.

Specifically, South African law uses the *lex specialis* principle, favouring more specific laws over general ones in cases of conflict. Therefore, existing laws could be adapted for AI-related issues, which might be more efficient than creating new *sui generis* regulations. Amending existing laws offers flexibility and adaptability for the evolving AI landscape and maintains legal coherence.

Enacting *sui generis* regulations for AI could be less comprehensive and slower than adapting broader frameworks. It could also lead to a disjointed legal environment where AI risks are addressed in isolation. Technology-neutral laws, adaptable to the dynamic AI landscape, could be modified to address AI-specific issues effectively.

Drafting new laws is time-consuming and expensive. With a lack of awareness of AI in both country's populations, investing in new *sui generis* legislation might not be an efficient use of resources. Furthermore, as AI evolves, laws specifically for AI might become outdated or inconsistent with other technologies.

Public participation in law-making is essential, but the limited public awareness of AI could lead to legislation that doesn't fully represent public interests. As developing countries, Kenya and South Africa might benefit more from enhancing existing laws for AI rather than creating new frameworks.

Applying principles like product liability to AI can provide predictability and control without needing new regulations. Sector-specific codes of conduct or innovation sandboxes could offer tailored guidance and flexibility.

Current AI-related regulations are fragmented across various laws without a cohesive strategy. This may lead to gaps in addressing AI-issues. However, there is no universal agreement on the nature of AI regulation, with debates around risk- or rights-based approaches remaining. South Africa's socio-economic landscape suggests that adopting legislative models from the EU or the US isn't feasible due to contextual differences. Hence, governance is crucial in ensuring equitable wealth distribution and mitigating unemployment due to AI deployment.

In conclusion, while Kenya and South Africa's legal frameworks address AI risks to some extent, adapting and extending existing laws could be more effective than creating new *sui generis* AI legislation. This approach would be more immediate, adaptable, and less resource-intensive, leveraging the current legal foundation while ensuring safety and accountability in AI technologies.

Kenya

AI Legislation in Kenya: Learning from Past Experiences

Evidence indicates Kenya faces a dilemma in regulating AI. The process of enacting the Information Communication and Technology Bill, 2020, and the proposed Kenya Robotics and Artificial Intelligence Society Bill, 2023, reveals industry scepticism towards government regulation of the ICT sector. Meanwhile, the President advocates for legislation to boost Kenya's AI competitiveness. However, it's uncertain if industry players align with this governmental approach.

Information Communications Technology Practitioners Bill, 2020

The Information Communication and Technology Practitioners Bill 2020 (ICT Bill), introduced in Kenya's National Assembly on November 20, 2020, faced significant controversy. This was not its first introduction, with previous attempts in 2016, 2018, and 2020 failing. The Bill proposed establishing an ICT Practitioners Institute, along with the registration and licensing of ICT practitioners. However, the Bill's broad definition of ICT practice and stringent qualifications for ICT practitioners, including a relevant bachelor's degree or diploma and demonstrated expertise, raised concerns. Many in the ICT sector feared being excluded due to these high standards.

Despite passing in the National Assembly, the Bill faced strong opposition, including an online campaign and criticism from Kenya's ICT Ecosystem Stakeholders, leading to its rejection by the president. Critics argued the Bill created unnecessary barriers to entry in the ICT industry, lacked stakeholder involvement, and threatened job creation and investment in SMEs and startups.

The ICT Bill's experience underscores the sector's preference for self-regulation over government intervention. The fluid nature of the ICT and AI sectors suggests that rigid legislation may hinder innovation and erect barriers, potentially stifling the use of these technologies.

The Kenyan Robotics and Artificial Intelligence Society Bill, 2023

The 2023 Kenya Robotics and AI Society Bill (AI Bill) mirrors the challenges faced by the ICT Bill. It reached Parliament through a public petition by the Kenya Robotics and AI Society, a non-profit organisation dedicated to advancing robotics and AI in Kenya. Interestingly, the Bill's creators claim to have utilised ChatGPT to generate a draft, which they then edited and submitted to Parliament. They argue that the Bill will foster skilled workforce growth, responsible innovation, and sustainable development if enacted.

Despite its potential benefits, the Bill encountered strong opposition from AI Kenya, an East African community comprising over 2,500 members, including machine learning and data science practitioners, business leaders, government officials, and enthusiasts. AI Kenya believes the Bill would create entry barriers for AI in Kenya, hindering its contribution to the tech ecosystem and economy. Ironically, the Bill aims to establish a professional body overseeing AI practitioners, introduce licensing fees, and secure government funding for AI research and development.

Nonetheless, on November 29, 2023, the Speaker of the National Assembly referred the Petition to the Public Petitions Committee for review under Standing Order 208A. The Committee evaluates the Petition and presents its findings to the House and the Petitioner as outlined in Standing Order 227(2).

South Africa

Alternative Approach to sui generis AI Legislation

South Africa's current AI-related legislative provisions have gaps and oversights. A multidisciplinary approach is needed instead of a consolidated *sui generis* AI legislative framework. Lyons emphasises the need for a tailored approach to governance due to diverse cultural, contextual, and historical factors across regions.

From a broad perspective, South Africa's AI governance should include safeguards for ethical and legal AI risks, guided by UNESCO's Recommendation on the Ethics of Artificial Intelligence, as South Africa is a UNESCO member. As a G20 member, South Africa should also consider G20 AI principles aligned with the EU's 'trustworthy AI' framework and ethical commitments like DeepMind's.

To ensure accountable and trustworthy AI applications without sacrificing human rights, regulatory bodies in South Africa should mitigate adverse external effects in areas like competition, privacy, safety, and responsibility. Brand suggests integrating algorithmic impact assessments into the legal framework, following King report principles, and appointing a data protection authority to address sector-specific challenges.

South Africa faces unique AI risks such as disinformation, inequality, and human rights violations. While the ideal regulatory framework is unclear, amending existing AI-related legislation and embracing smart regulation can be beneficial. Smart regulation involves a multi- stakeholder approach, allowing flexibility to adapt to AI's dynamic landscape, ensuring practical and relevant regulations, and harnessing diverse expertise for comprehensive and balanced AI governance.

Further Development of Existing Frameworks

As a developing country, South Africa should prioritise AI regulation due to potential human rights violations and ethical concerns. Instead of enacting *sui generis* AI regulations, a better approach is to amend existing AI-related provisions, gradually integrating them into relevant legislative frameworks through selective amendments.

A sector-specific approach is appropriate, particularly in high-risk sectors like healthcare, where ethical concerns are prominent. This approach aligns with other jurisdictions like Germany and France, which amend civil and labour codes to regulate AI applications in specific contexts. Rather than restricting innovation with central AI regulators, South Africa should formulate distinct sector-specific approaches within their existing authority.

Data privacy and personal data processing are somewhat regulated through POPIA, but additional provisions like compulsory labelling for AI systems can enhance transparency and compliance.

Regarding AI systems as inventors, the Patents Act should include a substantive examination step clarifying that AI systems cannot be inventors. The entity or organisation operating the AI system should be the designated patent applicant.

South Africa can enforce the constitutional prohibition against discrimination based on various grounds to address bias issues, mitigating bias associated with AI systems.

Establishing basic AI principles such as data prediction, fairness, accountability, and innovation, as done in Japan, and appointing a supervisory authority like India can guide ethical and responsible AI practices in alignment with South Africa's unique societal and ethical considerations.

Regulatory Sandboxes

In developing countries like South Africa, regulatory sandboxes are essential tools to bridge the gap between AI policy and regulation and the practical implementation of AI solutions. These sandboxes facilitate supervised testing of new technologies, generating valuable data for evidence-based policymaking. Several African nations have adopted regulatory sandboxes, acknowledging the challenges posed by AI's dynamic nature, diverse applications, and limited regulatory resources.

A regulatory sandbox is a controlled setting established by regulatory authorities, allowing private entities to experiment with new products under specific exemptions. It has become a mainstream method for assessing the feasibility and compliance of new AI solutions. With the necessary prerequisites for a regulatory sandbox, South Africa can collaborate with other developing countries, like those in the African Union, to formulate principles for sandbox implementation within their jurisdictions. Prioritising national priorities through thematic regulatory sandboxes is advisable to maximise resource efficiency.

Drawing from France and Italy, testing in sandboxes should be considered when assessing compliance with regulations and replicating real-world scenarios. This approach enhances regulatory assessments and stimulates innovation across various sectors.

Regulatory sandboxes streamline AI product commercialisation, reduce time and cost barriers, and equip regulatory bodies with the knowledge needed to adapt regulations to AI advancements. They encourage broader market participation, particularly for small- and medium-sized enterprises (SMEs), contributing to standards development and benefiting businesses, consumers, and the overall AI ecosystem.

Regulatory sandboxes prioritise user privacy by enabling private enterprises to introduce AI products aligned with data protection from the outset, addressing potential user manipulation. These sandboxes work hand in hand with innovation hubs, which have a broader scope and provide guidance on regulatory issues. South Africa’s tech hubs play a crucial role in fostering AI and digital technology growth but require a unique AI governance approach tailored to the African landscape.

Integrating innovation hubs into South Africa’s smart AI regulatory approach, as seen in Colombia, will expand the participation of institutions from various sectors in regulatory experiments, promoting economic development and digital transformation beyond the scope of sandboxes.

Part E: Key Findings and Recommendations

Inadequacies in Current AI-Related Legal Frameworks

Both the Kenyan and South African legislative frameworks reveal partial ability to address concerns related to AI shortcomings. For example, within the South African Consumer Protection Act, consumers may struggle to identify faults related to AI due to technical complexity or opaque algorithms. Therefore, specific guidelines and mechanisms within the Act are needed to assist consumers in recognising and addressing AI-related defects and harms.

Both legal frameworks already address various aspects of AI-related risks, encompassing data protection, consumer rights, and digital and consumer-related issues. Adapting and amending these laws to address AI-specific concerns could be more efficient than creating new *sui generis* AI regulations. AI is a rapidly evolving technology, and comprehensive legislation might struggle to keep pace, leading to suboptimal solutions, inadequate oversight, and legal uncertainties. Amending existing laws provides flexibility to accommodate AI's evolving landscape, particularly considering the lengthy law-making process.

To foster a more agile and forward-looking regulatory environment, sector-specific codes of conduct, guidelines, and innovation sandboxes developed by industry stakeholders and regulatory authorities can be implemented without immediate legislative changes.

AI is an interdisciplinary technology spanning multiple sectors and legal domains. Sui generis AI regulation could lead to fragmented legislation isolating AI-related challenges from broader lawful principles. Therefore, integrating AI concerns into existing legal categories ensures a holistic approach, maintaining consistency and predictability through established legal principles like product liability.

Considering the lack of public awareness of AI, drafting *sui generis* AI legislation without broad public understanding may not adequately represent public interests, potentially undermining democratic and inclusive principles.

From a financial perspective, introducing a *sui generis* legislative framework requires substantial time and resources. It would be more beneficial to allocate limited financial resources to strengthen existing laws addressing AI-specific concerns rather than creating an entirely new legislative framework.

Key Elements of AI Legislation to Ensure Responsible and Innovative Use of AI

Both Kenya's and South Africa's current legislative framework partially addresses AI risks but falls short of effectively accommodating these technologies' dynamic and nuanced nature. Thus, certain amendments are warranted. Ethical considerations should take centre stage, addressing concerns about bias, transparency, fairness, and accountability in AI technologies. Regulatory bodies should incorporate insights from international principles and frameworks into the approach. Identifying industries with high AI potential and supporting them through coordinated AI strategies, utilising local expertise and resources, is imperative for stimulating economic growth.

Additionally, incorporating algorithmic impact assessments into AI legal frameworks ensures the consideration of potential societal impacts and external effects. Appointing a specialised data protection authority for AI and involving the public in the regulatory process promote transparency and accountability, aligning with governing principles. Furthermore, exploring smart regulation as an alternative to traditional approaches acknowledges the dynamic nature of AI technologies and the need for adaptable regulations, striking a balance between innovation and risk mitigation.

Kenya

While current Kenyan laws are fragmented, they address various AI aspects, and any gaps can be addressed through amendments. Here are the recommendations:

1. Amend security and surveillance laws to regulate digital tools like facial recognition algorithms, ensuring due process and protecting fundamental rights.
2. Revise the Copyright Act to clarify AI-created works' copyright protection status and introduce exemptions to accommodate technological advancements, particularly in text and data mining. Consider the Intellectual Property Bill 2020 to address AI's impact on intellectual property.
3. Develop an AI Strategy to promote innovation in Kenya.
4. Implement regular sector-specific assessments to gauge AI's impact, providing a foundation for potential *sui generis* legislation.
5. Provide soft laws, such as guidelines, to promote predictability in ethical AI, even though they may not be legally binding.

South Africa

1. Specific guidelines and mechanisms within the Consumer Protection Act are needed to assist consumers in recognizing and addressing AI-related defects and harms.
2. Require the disclosure of AI algorithm logic to enhance transparency and facilitate bias detection.
3. A more robust examination process, including substantive examination to ensure alignment with the Patent Act's scope.
4. Specific guidelines for AI-related medical devices must be created to ensure post-deployment surveillance.
5. Clarity is needed with regard to electronic transactions to prevent contractual misunderstandings caused by AI-amended terms. Ambiguities regarding liability for automated transactions must also be addressed to avoid potential contractual evasion.

Conclusion

AI permeates various social, legal, political, and economic facets. While it offers numerous benefits, it also presents significant challenges. Hence, it is crucial to establish a comprehensive legal framework for AI regulation. Both Kenya and South Africa have laws that address AI adequately, these laws contain gaps that could be rectified through amendment. Regular sectoral assessments are essential to ensure that existing laws remain aligned with the evolving AI landscape, ultimately striving for a legal framework that promotes innovation and safeguards fundamental rights effectively.

List of Authorities

European Union

- *Regulation (EU) 2023/655 of the European Parliament and of the Council of 14 June 2023 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act).*

Statutes

Kenya

- *Computer Misuse and Cybercrimes Act, 2018.*
- *Copyright Act, 2001.*
- *Constitution of Kenya [Kenya], 27 August 2010.*
- *Consumer Protection Act, 2012.*
- *Data Protection Act, 2019.*
- *Health Act, 2017.*
- *Industrial Property Act, 2001.*
- *Information and Communications Act, 1998.*

South Africa

- *Constitution of the Republic of South Africa Act 108 of 1996.*
- *Consumer Protection Act, 68 of 2008.*
- *Electronic Communications and Transactions Act 25 of 2002.*
- *Medicines and Related Substances Act 101 of 1965.*
- *Patents Act 57 of 1978.*
- *Protection of Personal Information Act 4 of 2013.*

This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organisation for their continued support.

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

ARTIFICIAL
INTELLIGENCE
FOR
DEVELOPMENT
AFRICA

Sida