SHAPING THE FUTURE OF ICT INDUSTRY IN KENYA: A COMPARATIVE BEST PRACTICE OF REGULATING ICT PROFESSIONALS

Victor Otieno Agolla.

International Academic Journal of Information Systems and Technology (IAJIST) | ISSN 2518-2390

Received: 13th June 2024

Published: 17th June 2024

Full Length Research

Available Online at: https://iajournals.org/articles/iajist_v2_i1_358_372.pdf

Citation: Agolla, V. O. (2024). Shaping the future of ICT industry in Kenya: A comparative best practice of regulating ICT professionals. *International Academic Journal of Information Systems and Technology, 2*(1), 358-372.

ABSTRACT

The ICT industry is rapidly evolving, turning the world into a global village. This growth presents challenges and opportunities, with cybersecurity threats being a major concern. Collaboration between governments, businesses, and individuals is crucial to protect sensitive data and prevent cyber-attacks. Regulation of the ICT sector is essential to manage risks effectively. By implementing and enforcing policies and laws, standards are set for both providers and users of ICT services. This paper reviews laws, regulations, and policies from other countries to provide insights for countries like Kenya in regulating ICT professionals. The aim is to offer guidance for decision-making in Kenya's efforts to regulate the ICT industry, ensuring inclusivity and addressing risks. This paper delves into the importance of understanding the benefits, challenges, and success stories of regulating ICT professionals in other countries to help Kenya develop effective strategies for enhancing its own industry. By comparing Acts, challenges, recommendations, and conclusions related to the observed case, valuable insights are provided for countries like Kenya seeking to regulate ICT professionals. The review of laws, regulations, and policies implemented by other nations offers a comprehensive understanding of how to navigate the complexities of regulating ICT professionals. By learning from the experiences of other countries, Kenya can tailor its approach to regulation to suit its unique needs and challenges, ultimately fostering growth and innovation in the industry.

Key words: Act, Regulation, Policy, Responsible, Ethically.

INTRODUCTION

The global landscape is experiencing rapid evolution and transformation due to advancements in information and communication technology (ICT) (Zhang & Zhang, 2020). This evolution has turned the world into a closely connected village, where distance and time are no longer barriers. The ICT industry has witnessed exponential growth, attributed to the continuous development of innovative software and hardware solutions. Moreover, the integration of artificial intelligence and machine learning has further propelled this growth, revolutionizing the way we live, work, and interact. As a result, digital transformation has become a driving force across various sectors, reshaping businesses and societies alike. Not only has it revolutionized the way businesses operate, but it has also brought about significant societal changes. Individuals can now connect, collaborate, and access information like never before, breaking down barriers and enabling a more interconnected world.

The accessibility of smartphones, fast internet, and cloud computing has resulted in the easy availability of information, breaking down geographical limitations and promoting worldwide connectivity. As a result, businesses now have the opportunity to broaden their horizons and explore untapped markets. Additionally, the ICT industry has played a significant role in introducing groundbreaking technologies like the Internet of Things (IoT), big data analytics,

and virtual reality, which are revolutionizing sectors such as healthcare, transportation, and education, among others (Vermesan & Friess, 2022). Similarly, the utilization of ICT has simplified government service delivery and facilitated data consolidation.

As the ICT industry continues to evolve, it presents both challenges and opportunities. Cybersecurity threats have become a major concern, requiring constant vigilance and robust measures to safeguard sensitive data and protect against cyber-attacks (Rikalovic, Suzic, Bajic & Piuri, 2021). Moreover, the rapid pace of technological advancements necessitates a workforce that is capable of adapting to and embracing new technologies. This requires investments in education and training programs to equip individuals with the essential skills needed to succeed in the digital era (Bécue, Praça, & Gama, 2021). To fully harness the benefits of the ICT industry, governments, businesses, and individuals must collaborate and address the potential risks while ensuring inclusivity for all.

Regulating the ICT sector is crucial in addressing risks associated with technology. By implementing and enforcing critical policies and laws, both providers and users of ICT services are required to adhere to certain standards (Malhotra, Singh, Anand, Bangotra, Singh & Hong, 2021). This ensures that the industry operates safely and securely, protecting both individuals and organizations from potential threats. Examining the laws, regulations, and policies implemented by other countries can provide valuable insights for countries like Kenya looking to regulate ICT professionals. Understanding the benefits, challenges, and success stories of regulating ICT professionals in other nations, if any, can help Kenya develop effective strategies to enhance the industry within its borders.

By reviewing the experiences of other countries in regulating the ICT sector, Kenya can learn from the different approaches used. This knowledge can be used to tailor regulations that are suitable for the local context, taking into account the specific challenges and opportunities present in the Kenyan ICT industry. Additionally, studying the effect of regulations on ICT professionals in other countries, if any, can help Kenya anticipate potential obstacles and develop strategies to overcome them. Through adopting best practices and lessons learned from other nations, Kenya can create a regulatory framework that promotes innovation, growth, and sustainability in the ICT sector.

Furthermore, the paper provides an in-depth analysis of the policies, regulations, and laws that are currently enforced in the countries under study, juxtaposing them with the measures that Kenya has adopted to promote the responsible utilization and implementation of Information and Communication Technology (ICT). By drawing parallels with the experiences of other countries, the paper offers a comprehensive overview of the regulatory landscape in the field of ICT, paving the way for informed decision-making and strategic planning on whether there is a need to regulate ICT professionals in this digital age.

Comparison of Regulations Related to ICT

Country	Acts	Advocates	Purpose
Netherlands, Singapore, Kenya Singapore South Africa	• Personal Data Protection Act • Data Protection Act • Data Protection Trustmark (DPTM) Scheme • Protection of Personal Information Act	Establish a framework that governs the collection, storage, processing, and sharing of personal information, with the objective of protecting individuals' privacy rights and preventing unauthorized access or misuse of their data.	These Acts do not aim to regulate ICT professionals. They advocate for the responsible and ethical handling of personal information in the context of ICT use.
Netherlands, Singapore	Telecommunications Act	This Act aims to ensure fair competition, protect consumer rights, and promote efficient and reliable communication services..	In both countries, the Act does not aim to regulate ICT professionals. It aims to foster innovation, enhance connectivity, and create a conducive environment for the growth of the ICT sector.
Netherlands, South Africa Kenya	• Electronic Communications Act, • Electronic Communications and Transactions Act • Kenya Information and Communications Act (KICA)	These Acts are designed to provide legal certainty and protection for electronic transactions, data privacy, and security in information and communication technologies (ICT).	The aim of these Acts is to create a conducive legal environment that promotes trust, transparency, and efficiency in electronic communications and transactions, thereby fostering innovation and economic growth in the digital age.
Netherland Kenya	• Data Protection Authority (CBP) • Office of Data Protection Commission (ODPC)	These authorities ensure the protection of personal data and privacy rights of individuals.	They aim to create a secure and trustworthy environment for the processing and handling of personal data in the digital realm.
Netherlands	• National cyber security center	Serves as an authoritative body with the primary objective of safeguarding the security and integrity of ICT systems.	This authority aims to protect the digital infrastructure of the country from cyber threats and ensure the resilience of critical ICT systems.
Netherlands	• Digital Market Act	Regulate and promote fair competition in the digital market by addressing issues such as platform dominance, data access, and interoperability.	Ensure that digital platforms do not engage in anti-competitive practices and that smaller businesses have equal opportunities to thrive in the digital economy.

Singapore	• Electronic Transactions Act	Provides legal recognition and validity to electronic transactions, ensuring that they are legally binding and enforceable.	It provides a legal framework for electronic contracts, signatures, and records, promoting the use of electronic commerce and facilitating digital transactions.
	• Payment Systems (Oversight) Act	Regulate and oversee payment systems to ensure their safety, efficiency, and integrity.	It provides rules and standards for payment systems, promotes consumer protection, and fosters confidence in electronic payment methods (digital payments).
	• E-commerce Regulations	Provides a legal framework for electronic commerce, addressing issues such as consumer protection, electronic contracts, and online marketing.	Seeks to promote trust and confidence in online transactions, protect consumers from fraudulent practices, and ensure fair business practices in the digital marketplace
South Africa	• Prevention of Electronic Crimes Act	Provides legal provisions and penalties to deter and punish offenders, safeguarding individuals and businesses in the digital age.	It aims to aims to address and prevent various forms of electronic crimes, such as cyberbullying, hacking, identity theft, and online fraud.
Netherlands and EU countries	• General Data Protection Regulation	Sets out rules for the processing of personal data and aims to give individuals more control over their own information.	Require organizations to implement measures to ensure the security and confidentiality of personal data, as well as to obtain explicit consent before collecting and processing such data.
Netherlands	• Cybercrime Act	Provides a legal framework to prosecute individuals or groups involved in cybercrimes such as hacking, identity theft, and online fraud.	The Act aims to protect individuals, businesses, and the government from the increasing threats posed by cybercriminals.
Singapore	• Cybersecurity Act	Provides regulatory framework to ensure the security and resilience of essential services in the digital age	To strengthen the protection of sensitive data, promote cybersecurity awareness, and facilitate information sharing between public and private sectors.

	• Cybersecurity Strategy (2018)	It focuses on three key pillars: building a resilient infrastructure, creating a safer cyberspace, and developing a vibrant cybersecurity ecosystem.	Aims to mitigate cyber threats, protect critical information infrastructure, and ensure the secure and reliable use of digital technologies
Singapore South Africa	• Internet and Digital Media Division • Infocomm Media Development Authority (IMDA) Act (2016) • Information Technology Act	Establish guidelines and frameworks for the management of online content, data protection, cybersecurity, and electronic transactions, among other things	aim to regulate and govern the use of digital media and information and communication technologies (ICT) as well as promoting innovation and economic growth in the digital sector.
South Africa	• Film and Publications Board Act	Regulate and control the distribution, exhibition, and possession of films, publications, and interactive computer games.	Ensure that content disseminated through digital platforms adheres to certain standards and guidelines, particularly in terms of age restrictions, explicit material, and harmful content.
South Africa	• National Internet Exchange Point (NIXP)	Facilitate the efficient exchange of internet traffic between internet service providers (ISPs)	Aims to improve the speed, reliability, and cost-effectiveness of internet connectivity for end-users
Kenya	• Post and telecommunications Act (1998)	Establish guidelines and provisions for the efficient and effective management, operation, and development of postal and telecommunications services.	Aims to ensure the smooth functioning and growth of the post and telecommunications sector in Kenya, while adapting to the advancements and challenges brought about by the digital age
Kenya	• The Computer Misuse Act	Establishes legal framework, that protect the integrity, confidentiality, and availability of computer systems and data, as well as safeguard the interests of individuals and organizations	Aims to address and combat various forms of computer-related offenses and cybercrimes that have emerged with the rapid advancement of technology.
Kenya	• Consumer Protection Act	It is a legal framework that ensures fair and transparent practices in the digital marketplace, protecting consumers from fraudulent activities, misleading advertisements, and unfair contractual terms.	promote consumer confidence and trust in digital transactions by providing mechanisms for dispute resolution, enforcement of consumer rights, and the imposition of penalties for non-compliance.

Kenya	• Evidence Act (2011)	A comprehensive legal framework that governs the admissibility and authenticity of electronic evidence in Kenya	Aims to promote trust and confidence in the use of electronic evidence by setting standards for its reliability and authenticity, thereby enhancing the efficiency and effectiveness of the judicial system in the digital age

Observations Made

Several countries, such as the Netherlands, Singapore, and South Africa, have established regulations to govern activities concerning the use and implementation of Information and Communication Technology (ICT). These regulations are designed to ensure that ICT is employed responsibly and ethically, safeguarding the interests of individuals, businesses, and the government alike. The primary objective of these regulations is to encourage the appropriate utilization of ICT while also addressing any potential risks and challenges that may arise due to its widespread use.

Apart from promoting the responsible use of ICT, these regulations also seek to safeguard the privacy and security of individuals' data. Given the increasing volume of personal information being stored and shared online, countries must have mechanisms in place to prevent data breaches and cyber-attacks. Through the implementation of regulations that mandate organizations to comply with stringent data protection protocols, these countries are striving to establish a more secure and protected digital landscape for their populace.

Drawing from the experiences of other nations, the focus of existing Acts is primarily on overseeing the activities associated with ICT itself, rather than on regulating the professionals operating within the industry. This approach is adopted because the field of ICT is open to individuals from various educational backgrounds who can acquire the necessary expertise to participate in the sector. As a result, these regulations are designed to govern the activities linked to ICT, ensuring that technology is utilized in a manner that benefits society as a whole, irrespective of whether the individuals involved possess formal training or not.

By prioritizing the regulation of ICT activities over ICT professionals, the evidence gathered from the Acts analyzed indicates that these countries are able to establish a framework that is adaptable and responsive to the rapidly changing landscape of technology. This approach fosters innovation and expansion within the ICT industry by encouraging contributions from individuals with diverse backgrounds towards the advancement and implementation of ICT solutions. Ultimately, the objective of these regulatory measures is to strike a harmonious balance between promoting the responsible use of ICT and cultivating a vibrant and inclusive environment conducive to technological progress.

Other nations also have legislation in place that tackles digital literacy and technology access concerns. These countries are committed to promoting responsible and ethical use of ICT, while also working towards narrowing the digital divide and ensuring equal opportunities for all to benefit from technological progress. They are implementing various initiatives, including training programs to enhance digital skills and make technology more affordable and accessible. The ultimate goal is to foster an inclusive society, where every individual has the chance to actively participate in the digital economy.

Challenges of Regulating ICT Professionals

Despite efforts by countries to regulate activities related to ICT, most have chosen to focus on ensuring responsible use and application of ICT rather than regulating ICT professionals. One of the primary reasons for the lack of regulation in the ICT sector is that individuals working in this field, such as ICT service providers, software developers, and data handlers, do not necessarily fall under the category of traditional professionals like doctors or lawyers. The ICT industry is open to anyone who acquires the necessary knowledge and skills, making it challenging to impose strict regulations on professionals in this field. Furthermore, the diverse nature of the ICT sector allows individuals from various educational backgrounds to enter the industry and contribute their skills and knowledge. This diversity in the ICT workforce poses a challenge for countries looking to establish uniform regulations that can effectively cover all professionals in the sector. Unlike more regulated professions, ICT professionals come from a wide range of backgrounds, making it difficult to create standardized regulations that apply to everyone in the field. However, this flexibility in the ICT industry also brings benefits, as it allows countries to tap into a diverse pool of talent and ideas.

By welcoming individuals from different educational backgrounds into the ICT sector, countries can promote innovation and growth in the industry. This approach fosters creativity and encourages the development of new technologies and solutions, ultimately benefiting the overall advancement of the ICT sector. Unlike more regulated professions, ICT professionals come from a wide range of backgrounds, making it difficult to create standardized regulations that apply to everyone in the field. However, this flexibility in the ICT industry also brings benefits, as it allows countries to tap into a diverse pool of talent and ideas. By welcoming individuals from different educational backgrounds into the ICT sector, countries can promote innovation and growth in the industry. This approach fosters creativity and encourages the development of new technologies and solutions, ultimately benefiting the overall advancement of the ICT sector.

The decision to regulate ICT professionals is heavily influenced by the dynamic nature of the industry. With technology constantly evolving and new advancements being made at a rapid pace, regulating ICT professionals would require continuous updates and changes to keep up with the latest developments. However, this would not only be time-consuming but also hinder innovation and progress in the sector. Therefore, it is important to strike a balance between regulation and allowing room for creativity and growth.

Moreover, many countries choose not to regulate ICT professionals due to the potential negative impact it may have on the economy. The ICT sector is a vital driver of economic growth and development in numerous countries. By keeping regulations minimal, countries can attract foreign investments, encourage entrepreneurship, and create job opportunities. Excessive regulation could deter businesses from operating in countries that impose strict regulations on ICT professionals, leading to a loss of economic potential and competitiveness. Additionally, countries may be hesitant to impose strict regulations on ICT professionals out of fear of stifling creativity and hindering the development of new technologies. By allowing a more flexible approach to regulating the sector, countries can foster an environment that encourages innovation and entrepreneurship in the ICT industry. This approach not only promotes economic growth but also ensures that the industry remains at the forefront of technological advancements.

Recommendations

In the current digital era, the regulation of ICT users and providers holds significant importance. Given the fast-paced evolution of technology, it becomes essential to establish a standardized framework that guarantees the proficiency and ethical behavior of these professionals. Through the implementation of appropriate legislation, a nation can create a fair environment where individuals possessing the required expertise, knowledge, and credentials are valued and relied upon by both employers and customers. Furthermore, regulation plays a crucial role in safeguarding the interests of consumers by ensuring that ICT professionals comply with industry norms and best practices. It serves as a mechanism to uphold accountability and transparency within the sector, as regulated professionals are obligated to abide by a set of ethical guidelines that dictate their conduct and decisions. This not only benefits the professionals themselves but also instills trust and confidence among stakeholders in the industry.

However, such regulation will hinder the innovation and advancement of ICT, with the majority keeping away from the advancement of ICT, its use, and even its application. This is due to the fear that such regulation may not be clear to the ICT user or ICT service provider. This will go against the government's call for a digital literacy society and will widen the gap in bridging the digital divide and promoting equal opportunities for all individuals to benefit from technological advancements. Through promoting responsible use of ICT, protecting individuals' data, and addressing issues related to digital literacy and access, countries like the Netherlands, Singapore, and South Africa are paving the way for a more sustainable and equitable digital future.

In Kenya, there are existing Acts that are meant to govern ICT activities, but they may not have effectively controlled certain ICT-related activities. The proposal to create an ICT bill specifically targeting ICT professionals does not address the issues and illegal activities associated with ICT. Therefore, this paper suggests the following solutions:

Despite having the Data Protection Act in place, Kenya faces challenges with organizations and individuals breaching the act by sharing personal data due to the lack of clarity on what constitutes "personal data." The Act also lacks specific mechanisms for organizations to follow,

resulting in varying approaches to safeguarding personal information. To address these issues, it is crucial to enhance the Data Protection Act by drawing insights from Singapore's Data Protection Trustmark (DPTM) and implementing similar standards and practices. This involves setting clear guidelines for data collection, processing, and storage, along with imposing strict penalties for non-compliance. Strengthening the DPA can involve introducing a Trustmark certification scheme that ensures organizations adhere to data protection standards. This can be achieved through a certification process that evaluates organizations' data protection practices, granting them a Trustmark upon compliance. Other measures to enhance the Act include creating a registry of certified organizations to promote transparency and accountability, providing incentives like tax benefits to encourage participation in the certification process, and integrating the Trustmark scheme into the DPA's enforcement mechanisms for more effective monitoring and compliance.

Furthermore, Kenya can benefit from adopting measures to enhance transparency, accountability, and user consent in handling personal information. Organizations and individuals dealing with personal data should clearly define what it entails and include a consent note declaring that the information will only be used for its intended purpose and not shared with any other party. By incorporating these strategies and practices, Kenya can strengthen its Data Protection Act, improve data protection standards, and enhance trust among organizations and individuals regarding the handling of personal information. Aligning with the principles of the DPTM can lead to a substantial enhancement in Kenya's data protection laws, thereby providing better protection for the privacy rights of its citizens. By following a comparable strategy, the DPA has the potential to elevate data protection standards in Kenya, fostering a culture of adherence and confidence among both organizations and individuals. This alignment with the principles of transparency, accountability, and security will guarantee the safeguarding of personal data in the modern digital age.

The Kenya Information and Communications Act (KICA) is responsible for overseeing the licensing and regulation of various telecommunications and internet service providers, as well as other information and communication services within the country. Despite the existence of this Act, there are still numerous instances where both companies and individuals are found to violate its regulations. One major issue is the rampant spread of fake news and misinformation, which is largely due to the absence of mechanisms to verify the authenticity of such information. Moreover, the lack of a legal framework for engaging in digital services or e-commerce has resulted in many individuals falling victim to online scams, leading to financial losses. This has forced citizens to resort to informal agreements when conducting online transactions, creating a loophole that scammers are quick to exploit. Consequently, this negative perception of online business as being rife with fraudulent activities has hindered the growth of e-commerce in the country. Drawing inspiration from the Electronic Communications and Transactions Act in South Africa, Kenya could potentially strengthen the provisions of KICA by introducing a requirement for individuals engaging in online business or publishing content to sign a consent form. This form would hold them legally accountable for any breaches of the law.

By incorporating similar measures to those outlined in the South African Act, such as mandatory data breach notifications, enhanced cybersecurity protocols, clear guidelines for digital signatures, and stricter penalties for cybercrime, Kenya could significantly improve the security and integrity of its digital transactions. Through the adoption of these provisions, KICA would establish a more comprehensive and robust framework for regulating electronic communications in Kenya. This, in turn, would help safeguard the interests of citizens and promote a safer online environment for conducting digital transactions. By aligning its regulations with international best practices, Kenya can enhance consumer confidence in e-commerce and combat the negative perception associated with online business transactions. Including measures for setting up and overseeing internet exchange points (IXPs) in Kenya, mirroring the NIXP framework in South Africa, the legislation has the potential to boost the effectiveness, accessibility, and safety of internet services within the nation. This initiative could stimulate domestic internet traffic exchange, minimize delays, and enhance internet access for individuals in Kenya.

The Office of Data Protection Commission (ODPC) in Kenya is an independent entity responsible for upholding data protection laws within the country. Despite its authority to regulate and enforce these laws, the ODPC has encountered challenges in issuing timely guidelines and regulations, as well as in investigating and prosecuting data breaches. One of the major obstacles faced by the ODPC is the limited availability of resources and capacity to effectively enforce data protection laws. This has resulted in many organizations disregarding these laws without facing consequences, thereby putting individuals' personal data at risk of being misused or exploited. To address these issues, it is crucial to establish clear guidelines, measures, and a standardized approach that both organizations and individuals must follow to comply with the Data Protection Act. It is essential to clearly define what constitutes personal data and provide organizations with the necessary tools to safeguard this information and prevent the unauthorized dissemination of personal details. Taking inspiration from the General Data Protection Regulation implemented in the Netherlands and other EU countries, Kenya could develop a similar law that empowers individuals to have more control over their personal information. This can be achieved by requiring organizations to obtain explicit consent before collecting and processing individuals' data, ensuring that individuals are aware of how their information will be used.

Kenya has witnessed a significant increase in the adoption of digital technologies and the growth of ICT infrastructure. As a result, there is a growing demand for reliable internet connectivity to support the high volume of digital activities. However, there is a stark contrast in the reliability of internet services provided by different organizations. While some offer highly reliable internet connections, others struggle to maintain a consistent and stable service. This discrepancy in internet reliability has led to certain companies dominating the sector, hindering the overall growth of ICT and creating a sense of monotony. To address this issue, it is crucial to establish a law, policy, or regulation that mandates internet sharing, especially in areas with limited internet coverage, such as rural regions. An excellent example of such a policy is the Digital Market Act of the Netherlands. By enforcing internet sharing, this initiative would encourage the widespread usage of ICT, foster the growth of small businesses, and

facilitate the delivery of digital services to every Kenyan. Furthermore, implementing such a regulation would promote fair competition within the industry and effectively tackle the problem of platform dominance. By ensuring that all organizations have equal access to reliable internet connectivity, the playing field would be leveled, allowing for a more diverse and competitive ICT sector in Kenya. Ultimately, this would contribute to the overall development and advancement of the country's digital landscape, benefiting both individuals and businesses alike.

The rise of online business and e-commerce in Kenya presents a promising opportunity for the growth of small businesses and the creation of job opportunities, especially for the youth. This surge in online activities addresses the issue of limited job prospects in the country. However, with the flourishing online marketplace comes the risk of exploitation by hackers and fraudsters who take advantage of unsuspecting citizens. Some individuals engage in fraudulent schemes, luring victims into fake businesses that require substantial financial commitments without disclosing the true nature of the transaction. This deceptive practice thrives due to the absence of specific legislation governing online business operations in Kenya. Drawing inspiration from established laws such as the Electronic Transactions Act and Payment Systems (Oversight) Act in Singapore, as well as the E-commerce Regulations in Singapore and the Prevention of Electronic Crimes Act in South Africa, Kenya has the opportunity to enact regulations that mandate transparency in online transactions. A proposed law could require parties involved in online business dealings to provide detailed information about the beneficiaries of transactions, including bank account details and a mechanism for tracing the flow of money.

Additionally, the implementation of a secure online/digital signature system would ensure the authenticity of transactions and serve as a legally binding document. By establishing a framework that enables the tracking of online transactions and the identification of involved parties, the incidence of theft and online scams could be significantly reduced. Furthermore, the introduction of stringent measures and legal consequences for fraudulent activities. This regulatory environment would foster a safe and trustworthy online marketplace, encouraging the growth of legitimate small businesses while discouraging fraudulent activities. Ultimately, the implementation of such laws would not only protect consumers but also facilitate a conducive environment for sustainable business growth in Kenya's digital economy.
Kenya has recently implemented the Computer Misuse and Cybercrime Act, which aims to address the growing issue of online crime and the malicious use of computers, such as the dissemination of defamatory information. However, there are concerns regarding the broad definition of cybercrime provided by the act, as it may be misused in court to falsely implicate individuals, including investigative journalists. To ensure clarity, it is crucial to clearly define the various dimensions of cybercrime.

Additionally, the act lacks sufficient mechanisms for transparency and accountability in the investigation and prosecution of cybercrime cases. This creates a potential for authorities to abuse their power and limits the ability of the accused to defend themselves. Furthermore, the act poses a threat to online freedom of expression and privacy, as it allows for the interception

of communications and the monitoring of online activities without a warrant. To address these issues, it is necessary to develop a comprehensive cybersecurity strategy, similar to the one adopted in Singapore, that can effectively mitigate cyber threats, protect critical information infrastructure, and ensure the secure and reliable use of digital technologies. By combining elements from the Internet and Digital Media Division of the Infocomm Media Development Authority Act (2016) in Singapore and the Information Technology Act of South Africa, a law can be formulated that strengthens the use of information and communication technologies (ICT) and enhances data protection, thereby fostering innovation and facilitating the growth of businesses.

The Evidence Act (2011) serves as a crucial document that establishes the regulations and processes governing the acceptance and presentation of evidence during legal proceedings. Its primary objective is to guarantee that the evidence introduced in court is dependable, pertinent, and permissible, thereby contributing to the delivery of fair and equitable legal judgments. Nevertheless, the Act lacks explicit directives concerning the admissibility and legitimacy of electronic evidence, resulting in ambiguities during court trials and the potential for miscarriages of justice. To address these shortcomings and adapt to the digital landscape, it is imperative to amend and update the Act by incorporating clauses that address the verification, gathering, preservation, and acceptance of electronic evidence. Furthermore, it is essential to include guidelines on the utilization of digital signatures, encryption methods, and electronic records to bolster the credibility and trustworthiness of electronic evidence in legal proceedings. Moreover, providing training sessions for legal practitioners and law enforcement entities on the proper handling of electronic evidence is paramount to ensure the effective implementation of the Act in the digital age. By enhancing the Act to encompass these aspects, the legal system can better navigate the complexities associated with electronic evidence and uphold the principles of justice and fairness in court proceedings.

To support the growth of online businesses in Kenya, it is important to establish a law that is comparable to the Electronic Transactions Act in Singapore. This law, which could be called the Electronic Communication and Transactions Act (ECTA), would serve to enhance the security and efficiency of electronic communication and transactions. By implementing this law, Kenya would have a more comprehensive and modern framework for electronic transactions, which would include regulations on electronic signatures, data protection, and online dispute resolution. For example, the Singaporean Act provides a clear definition of electronic signatures and allows for their use in place of traditional signatures. Kenya could adopt similar provisions to encourage the use of electronic signatures in contracts and transactions. Additionally, the Singaporean Act includes robust provisions on data protection, such as the right to access and correct personal data. Kenya could adopt similar provisions to safeguard the privacy of individuals in the digital age. Furthermore, the Singaporean Act also incorporates mechanisms for online dispute resolution, such as mediation and arbitration. Kenya could adopt similar provisions to facilitate the resolution of disputes more efficiently and cost-effectively. By enacting the Electronic Communication and Transactions Act, Kenya would be able to promote the use of electronic communication and transactions securely and efficiently, ultimately benefiting the growth of online businesses in the country.

The Central Bank of Kenya (Amendment) Act, 2016 can draw valuable lessons from the Payment Systems (Oversight) Act in Singapore. This act in Singapore serves as a comprehensive framework for overseeing payment systems, with a focus on ensuring their stability, security, and efficiency. To enhance the effectiveness of the Central Bank of Kenya (Amendment) Act, 2016, Kenya can consider implementing the following recommendations: First, establishing a dedicated body responsible for overseeing payment systems, similar to the Monetary Authority of Singapore's (MAS) Payment Systems Oversight Department. This body would be tasked with regulating and monitoring payment systems in Kenya, ensuring compliance with established standards and guidelines. Secondly, adopting a risk-based approach to oversight, prioritizing high-risk payment systems, and proactively addressing emerging threats. This approach would enable the identification and mitigation of potential vulnerabilities in the system. Thirdly, developing and implementing robust cybersecurity standards specifically tailored for payment systems. These standards would ensure the integrity and resilience of the systems, safeguarding them against cyber threats and attacks. Lastly, enhancing consumer protection by providing clear guidelines and regulations for payment service providers. This would promote transparency and accountability, ensuring that consumers are well-informed and protected when using payment services. By adopting these insights, Kenya can strengthen its payment systems, bolster financial stability, and foster a secure and efficient digital economy. Additionally, this Act would play a crucial role in combating fraud and illegal business activities, thereby reducing instances of money laundering and other criminal activities involving financial transactions.

Conclusion

Based on observations made regarding the need for formulating a law to regulate ICT professions in Kenya, it is evident that the task presents several challenges. One of the primary difficulties lies in the fact that individuals entering the ICT sector may not necessarily possess formal qualifications or professional certifications. This opens up the field to a wide range of individuals from diverse backgrounds, some of whom may lack the necessary expertise or ethical standards required in the profession.

Furthermore, the rapidly evolving nature of ICT, characterized by constant advancements and innovations, poses a significant challenge to the formulation of regulatory laws. Any legislation put in place would need to be regularly updated to keep pace with these changes. This would not only be time-consuming but could also result in laws that quickly become outdated and ineffective in addressing the dynamic landscape of the ICT sector.

Additionally, implementing strict regulations on ICT professionals could potentially stifle innovation and hinder the growth of small businesses, which are vital for job creation in the country. Such restrictions may also deter citizens from utilizing ICT services due to fear of legal repercussions, ultimately impacting service delivery to both government institutions and the private sector. Instead of focusing on regulating ICT professions, it may be more beneficial for the government and the Ministry of ICT to concentrate on strengthening existing laws that address criminal activities involving the misuse of ICT. This approach could help maintain a

balance between promoting responsible and ethical ICT use while also fostering innovation and job creation in Kenya.

REFERENCES

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), 1809.

Rikalovic, A., Suzic, N., Bajic, B., & Piuri, V. (2021). Industry 4.0 implementation challenges and opportunities: A technological perspective. *IEEE Systems Journal*, *16*(2), 2797-2810.

Vermesan, O., & Friess, P. (Eds.). (2022). *Digitizing the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*. CRC Press.

Zhang, X., & Zhang, Z. (2020). How do smart villages become a way to achieve sustainable development in rural areas? Smart village planning and practices in China. *Sustainability*, *12*(24), 10510.