KB SCHOLARS JOURNAL OF LAW
ISSN 3027-2440 (Online)https://kbsjournals.com/10.5281/zenodo.20774657
Published by KB SCHOLA RS JOURNAL
Vol. 4 Issue 3 [May-Jun]

www.growkudos.co
GoogleAnalytics
GoogleScholars
KBLSP Journal
Open Research Europe

# THE ROLE OF LAW IN NAVIGATING THE DIGITAL WORLD IN THE 21ST CENTURY

▪Seun Omowonuola Afolayan ▪▪ Olaide Awwal Bolanta ▪▪▪ Oluwaseun Ojo
▪ [Doctoral candidate] Bsc (Hons), Msc, LL.M, BL
<seun-omowonuola.afolayan@eksu.edu.ng> <https://orcid.org/0009-0008-4088-0969>
▪▪ [LL.M, B.L] Associate, Olaniwun Ajayi
<oawwal-bolanta@olaniwunajayi.net> <https://orcid.org/0009-0004-5216-0775>
▪▪▪ [LL.M. B.L] University of Notre Dame, USA
<oojo2@alumni.nd.edu> <https://orcid.org/0009-0004-8897-1924>

Received: 30/04/26 Revised: 10/06/06 Accepted: 17/06/26

DOI: 10.5281/zenodo.20774657

Abstract
The rapid evolution of digital technologies has transformed the way we live, work, and interacts. As we navigate this digital landscape, the role of law has become increasingly crucial in addressing the challenges and opportunities presented by emerging technologies. This paper examined the intersection of law and technology, highlighting the need for adaptive regulatory frameworks that balance individual rights and freedoms with the interests of businesses, governments, and society as a whole. The authors argued on the role of law in the 21st century as a tool to promote innovation, as well as provide a framework for responsible innovation that promotes trust, security, and fairness in the digital world and furthermore, to focus on data protection, cybersecurity, intellectual property, with digital rights and freedoms. The paper also explored the challenges posed by emerging technologies such as artificial intelligence, block-chain, and the Internet of Things.

Keywords: Law, digitalisation, artificial intelligence, block-chain, framework

©Terms and conditions of access and use can be found at https://www.kbsjournals.com/index.php/kblsp

## 1. Introduction

Envisioning routine human life without digital technology is almost impossible due to the huge reliance on contemporary civilisation on digital tech. With the introduction of computers in 1946 with ENIAC which were so large that they took up an entire room while able to perform only basic functions compared with the capabilities of the modern-day computers, the world has been largely dependent on the functionalities of technologies. After ENIAC, the first true personal computer was released, targeting a

more general audience.[1] Since then, there has been constant development and improvement on the functions, size, models, programs and even the capabilities, technology has developed from human-aided calculations to fully automated commanded functions,[2] from ENIAC to the introduction of the mobile phone in 1973, followed by the first laptop in 1981, the deployment of internet connectivity with the World Wide Web in 1991.[3]

Digital technologies have evolved remarkably over the past few decades, this has reshaped virtually every aspect of human life with the invention of Artificial Intelligence as a topmost change at the moment, from natural language processing to machine learning, AI systems are becoming increasingly sophisticated with high capabilities to revolutionise industries such as healthcare, finance, and transportation.[4] Block-chain technologies are another example of the development of digital technologies, block-chain technology which was initially introduced as the foundation for cryptocurrencies like Bitcoin is now being utilised for secure record-keeping, supply chain management, and smart contracts.[5] The proliferation of connected devices has enabled seamless integration between physical and digital environments, transforming homes, cities, and industries, hence the development of the concept of Internet of Things.[6] The development of internet networks from edge to 5G must not be swept aside as it marks a significant development in the world of technology, with the innovation of 5G networks which introduced high-speed internet connectivity, has paved the way for advancements in virtual reality, autonomous vehicles, and real-time communication. Furthermore, cloud computing and the ability to store and access vast amounts of data remotely has transformed business operations and enabled global collaboration has transform the business world.[7]

One of the most notable impacts of digital technology is the democratisation of information. The internet has made knowledge more accessible than ever, enabling

[1] Birmingham City University, "Digital Technology Then and Now" https://www.bcu.ac.uk/blog/computing/digital-technology-then-and-now> accessed 18 January 2025
[2] An example of this is the prevalence of Artificial Intelligence Technologies
[3] Matt Paige, "The Evolution of Digital Transformation History: From Pre-Internet to Generative AI" https://hatchworks.com/blog/product-design/history-digital-transformation/ accessed 18 January 2024
[4] Bajwa J, Munir U, Nori A, Williams B. Artificial intelligence in Healthcare: Transforming The Practice Of Medicine. Future Healthc J. (2021) Jul;8(2):e188-e194. doi: 10.7861/fhj.2021-0095. PMID: 34286183; PMCID: PMC8285156.
[5] Dong, Shi & Abbas, Khushnood & Li, Meixi & Kamruzzaman, Joarder. (2023). Block-chain technology and application: an overview. PeerJ Computer Science. 9. e1705. 10.7717/peerj-cs.1705.
[6] Kumar, S., Tiwari, P. & Zymbler, M. 'Internet of Things is a Revolutionary Approach For Future Technology Enhancement: A review' (2019) *J Big Data* **6**, 111 . https://doi.org/10.1186/s40537-019-0268-2
[7] Ibid

individuals from all corners of the globe to access educational resources, engage in civic discussions, and participate in cultural exchanges. This access has fostered a more informed and connected global citizenry. In the economic realm, digital technologies have revolutionised industries, creating new business models and job opportunities through E-commerce platforms that create remote work and allow for greater employment flexibility. While this functions as a great development, it has also widened the gap between those with access to digital tools and those without, emphasising the need to address the digital divide.[8]

Social media platforms, a product of digital technologies, have redefined communication, by allowing people to connect instantly across vast distances, thus, facilitating the exchange of ideas and the formation of online communities, they, however, have also given rise to challenges such as misinformation, cyberbullying, and the erosion of privacy. The impact of digital technologies on healthcare is also immense, ranging from telemedicine,[9] wearable health devices and AI-driven diagnostics, have improved access to medical care and enhanced patient outcomes. Nevertheless, these advancements have continuously raised questions, in recent times, about data security and the ethical use of medical information.[10]

Digitalisation has the potential to increase productivity, facilitate access to new markets, create new industries and jobs, improve service provision, increase people's well-being, and enable more sustainable production models with the environment. However, it can also mean new sources of social exclusion, greater concentration of wealth, and new risks in terms of security and data protection, as well as increased energy consumption, among others.[11] Despite its benefits, the pervasive influence of digital technologies has introduced significant challenges. Cybersecurity threats, such as hacking and identity theft, pose risks to individuals and organisations alike. Furthermore, the automation of jobs through AI and robotics has led to concerns about unemployment and economic

[8] World Bank Group, *Digital Progress and Trends Report* (2023) https://openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content accessed 18 January 2025

[9] Purnama, Yulian & Asdlori, Asdlori, 'The Role of Social Media in Students' Social Perception and Interaction: Implications for Learning and Education. Technology and Society Perspectives (2023) *TACIT*. 1. 45-55. 10.61100/tacit.v1i2.50.

[10] ibid

[11] United Nations, Digitalisation and Development: An Increasingly Stronger Link" https://desarrollodigital.cepal.org/en/digitalization-development> accessed 18 January 2025

displacement,[12] reports by groups such as McKinsey suggest that 800 million people could lose their jobs to automation by 2030, while polls reveal that the majority of all employees worry that they do not have the necessary training or skills to get a well-paid job[13], the unauthorised use of data and breach of data privacy, the proliferation of social media for financial benefits which result in loss to the unsuspecting viewers such as misleading advertisement, the abuse of the technology for academic purposes, and extreme technologies.

Advancements in digital technologies can be used to defend and exercise human rights but they can also be used to violate them, for example, by monitoring our movements, purchases, conversations and behaviours. Governments and businesses increasingly have the tools to mine and exploit data for financial and other purposes. Thus, personal data would become an asset to a person, if there were a formula for better regulation of personal data ownership. Data-powered technology has the potential to empower individuals, improve human welfare, and promote universal rights, depending on the type of protections put in place. These and many more effects of digital technology beg for the intervention and regulation of technology by law. Thus, this paper will discuss the importance of law in regulating digital technologies and the importance of keeping up to date with the advancement in technology.[14]

## 2. Nature and scope of the relationship between Law and Technology

As technology continues to outpace traditional regulatory mechanisms, these developments continue to highlight the urgent need for adaptive laws and regulations that are not only capable of addressing the challenges but can encourage innovation. Central to the intersection of law and technology is the need to balance individual rights and freedoms and accommodating the interests of businesses, governments, and society.

At this stage it is obvious to mention that the transformative power of technology has led to and its unprecedented challenges in legal governance. The advancements in

[12] Mateausz Brodowicz, "The Impact of Digital Technology on Modern Society and Economy" https://aithor.com/essay-examples/the-impact-of-digital-technology-on-modern-society-and-economy accessed 18 January 2025

[13] United Nations, 'UN75 2020 and Beyond: Shaping Our Future Together" https://www.un.org/en/un75/impact-digital-technologies#:~:text=Digital%20technologies%20have%20advanced%20more,can%20be%20a%20great%20equaliser. Accessed 18 January 2025

[14] United Nations, 'UN75 2020 and Beyond: Shaping Our Future Together"

technology such as the AI, block-chain, and the Internet of Things while they offer significant benefits also introduce complex legal questions concerning privacy, intellectual property, liability, and security and as such, this has left traditional legal frameworks, designed for static and slower-paced environments, struggling to address these rapidly evolving issues. This raises the concern and need for adaptive regulatory frameworks which are essential to keep pace with technological change. These frameworks must be flexible, technology-neutral, and forward-looking to anticipate future developments. For instance, AI's rise necessitates regulations that account for ethical considerations, bias mitigation, accountability, and transparency without stifling innovation. Similarly, the emergence of block-chain technology challenges traditional notions of jurisdiction, data ownership, and enforcement, demanding novel legal solutions.

The potential for the misuse and exploitation of technology become more pronounced as technology becomes more pervasive as data breaches, mass surveillance, and algorithmic biases pose significant threats to individual rights such as data protection rights[15] and rights against discrimination.[16] For example, facial recognition technology, while valuable for security purposes, raises concerns about privacy invasion and potential misuse by authoritarian regimes.[17] For example, on December 5, 2024, the ACLU and the ACLU of Michigan filed an amicus brief in *Woodruff v. Oliver*,[18] a wrongful arrest lawsuit in the United States District Court for the Eastern District of Michigan, arguing that the Detroit Police Department's (DPD) reliance on flawed facial recognition technology (FRT) impermissibly tainted the investigation and failed to establish probable cause for the plaintiff's arrest. This reiterates the importance of ensuring that technological advancements do not erode fundamental human rights.

Businesses use technology to innovate, increase efficiency, and compete globally. However, they confront difficulties negotiating a patchwork of legislation across jurisdictions, particularly in data protection and cybersecurity areas. Striking a balance between the several laws entails creating restrictions that are not unduly cumbersome while adhering to ethical and legal guidelines. Incentives for self-regulation and

[15] UDHR, CFRN, GDPR, NDPA
[16] UDHR, CFRN
[17] Clive Coleman, 'Police facial recognition surveillance court case starts' (BBC NEWS, 21 May 2019) https://www.bbc.com/news/uk-48315979 accessed 19 January 2025.
[18] *Woodruff v Oliver (http://aclu.org/cases/woodruff-v-oliver)*

adherence to industry best practices can supplement legislative measures, establishing a culture of accountability and ethical responsibility.

The role of government in ensuring the balance between law and technological progress, is thus, not only limited to promoting technological progress but also protecting citizens from the potential harms of technology. This duality of duty requires a nuanced approach. For instance, while governments may leverage AI for national security and public welfare, such as in predictive policing or healthcare diagnostics, they must ensure that these applications do not infringe on civil liberties or exacerbate inequalities. This can be seen in steps taken in some countries around the world to regulate technology and its effects. The General Data Protection Regulation[19], The Artificial Intelligence Act[20], the Nigeria Data Protection Act[21], the United Kingdom Data Protection Act[22] etc are laws that have been enacted both at national and international levels to deal with the effect of technology while ensuring that technology is not discouraged or disadvantaged.

The capabilities of technology also extend immensely to the societal level, it acts as a bridge in closing social gaps and creating immense opportunities for citizens. On the contrary, however, it can also deepen divides, particularly in developing regions with limited access to digital infrastructure. This is an area for intervention by legal frameworks to ensure that technological benefits are equitably distributed and do not exacerbate existing disparities.

It is therefore imperative that regulatory frameworks evolve hand-in-hand with technological advancements to support flexibility, collaboration, and forward-thinking policies.

# 3. Digital Technology and Key Areas of Concern in 21st Century

I. Data protection

Data protection encompasses the legal, ethical, and technical measures aimed at safeguarding personal data from unauthorised access, misuse, or breaches.[23] Personal

[19] The European Union General Data Protection Regulation, 2018
[20] The European Union Artificial Intelligence Act, 2024
[21] The United Kingdom Data Protection Act, 2023
[22] Data Protection Act 2018
[23] Chukwubuikem I Obianyo, Solomon V. Ater, 'The Legal Implication of Data Privacy and Protection in The Age of Big Data and The Ever-Emerging Technologies in Nigeria.' (2023) *Idemili Bar Journal*

data includes any information that identifies an individual, such as names, addresses, biometric data, or online behaviours. Protecting such data is crucial for maintaining individual privacy, upholding trust in digital systems, and preventing harm such as identity theft, discrimination, or reputational damage.

The terms data protection and data privacy are often used interchangeably as they seem to overlap because they both seek to protect the integrity of data and the individuals' interests in how their information is being used or processed. These terms are however different, in that, data protection aims to safeguard an individual's right to his data and refers to means employed to ensure that data is kept safe, secure, and guarded against unauthorised access, corruption, compromise, or loss. Data privacy, on the other hand, concerns itself with the administration and regulation of the use and dissemination of personal information.[24]

Data protection involves the regulation of the use, storage and processing of data by data processors or data controllers, and it involves safeguarding the rights of data subjects such as the right to be informed in a clear and concise manner, without unreasonable delay of the status of the data and whether or not it will be processed, the purpose of the processing and the categories of the recipients of the data. [25] it covers the right to rectification[26] and erasure,[27] the right to withdraw consent previously given,[28] the right to object to the processing of data,[29] the right not to be subject to a decision based solely on automated decision-making,[30] and the right to data portability.[31]

II. Cybersecurity

Cybersecurity can be defined as the application of technology to protect systems from cyber-attacks. Cybersecurity encompasses the measures, practices, and technologies designed to protect systems, networks, and data from unauthorised access, theft, damage, or disruption. While the term cybersecurity itself connotes the technical application of technological implements in ensuring the safety of cyberspace, its regulation is wholly

[24] A. Odusote, 'Nigeria: Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation,' In Beijing Law Review, Vol. 12. No. 4, December, 2022; available at <https://scirp.org/journal/paperinformation.aspx?paperid=114265>
[25] NDPA, section 34 (1); GDPR Article 15
[26] NDPA, section 34 (1) (v), GDPR Article 16
[27] NDPA, section 34 (1) (v), GDPR Article 17
[28] NDPA, section 35
[29] NDPA, section 36
[30] NDPA, section 37
[31] NDPA, section 38

dependent on cyber law which can be defined as the laws guiding the use of cyberspace. The security of cyberspace is of immense concern and importance these days where the use of the internet on a daily basis surpasses the use of other means of communication or socialisation. As digital transformation accelerates across sectors, the growing sophistication of cyber threats poses significant challenges to economic stability, national security, and individual privacy. A case in reference is the Equifax Breach of 2017, a cyberattack that resulted in the theft of personal information of over 140 million consumers from the Equifax network in a catastrophic data breach, including people's Social Security numbers, driver's license numbers, email addresses, and credit card information.[32] This event led to the loss of public trust in Equifax, generated a lot of backlash and the company faced significant financial repercussions, including a settlement of up to $700 million with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories. The settlement included compensation for affected consumers, regulatory fines, and legal fees.[33] Another example of the devastating effect of cyberattacks is the Costa Rica ransomware attack that happened in 2022, a malware attack on 27 different public institutions in Costa Rica by two groups named Conti and Hive Groups respectively. The attack was carried out in sequence while demanding Twenty Million Dollars ($20,000,000). The Costa Rica Government refused to pay the ransom as it saw it as a terrorist attack so the websites were down from May 2022 and continued till June 2022, during this period, the government was forced to make some strategic decisions which caused the country to lose up to $125,000,000 (One hundred and Twenty-Five Million US Dollars).[34] The gravity of loss likely to occur to individuals, bodies or governments due to cyberattacks buttresses the importance of cyber security and the need for strict regulation, enforcement of laws and punishment of offenders to safeguard cyberspace.

## III. Intellectual property

Intellectual Property (IP) refers to the legal rights of creators and innovators for their inventions, artistic works, trademarks, and designs. However, as technology advances, the traditional IP frameworks are increasingly challenged, and this has continually raised

[32] Srinivasan, Suraj, Quinn Pitcher, and Jonah S. Goldberg. "Data Breach at Equifax" Harvard Business School Case 118-031, October 2017. (Revised April 2019.)
[33] Breach Sense, 'Equifax Data Breach: A Case Study' https://www.breachsense.com/blog/equifax-data-breach/ accessed 21 January 2025
[34] Editorial, 'Costa Rica Ransonware Attack' https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022) accessed 21 January 2025

concerns about infringement, enforcement, and the balance between protection and accessibility. IP infringement is the violation of the rights of IP creators which starts when a literary, artistic work or a trademark and industrial design protected by IP Laws is used, copied, pirated, or otherwise exploited without proper authorisation from the owner of the rights.[35]

While IP rights have been of immense value and advantage to the promotion of technological development by incentivising innovation such as granting digital creators exclusive rights to their innovations, facilitating economic growth and encouraging creativity, technology has also been of advantage to creators, individuals, government and bodies by providing platforms for dissemination and development of their ideas. However, along with these reciprocal benefits comes some point of concern. Digital piracy and copyright infringement are part of the concerns of IP rights in technology, the use of the internet has made it easier to copy and distribute works of creators, thus, undermining and affecting the proprietary and pecuniary interests of the creators, this is the case in *Oracle v Google* where Oracle sued Google for its use of APIs in its Android and that the act constituted copyright infringement, as Google had not obtained a license from Oracle to use the Java APIs in Android.[36] Another challenge is the impact of open-source software on intellectual property. The rise of open-source software, where developers share code freely for modification and personal use is a challenge to the main purpose of IP. While open-source promotes collaboration, it raises questions about how contributors' rights are protected and compensated.

Furthermore, the notion of IP rights surrounds the fact that the duty to trace IP infringement lies on the right holders who will then report or bring an action for enforcement of their right and to stop the continuation of such infringement, with the existence of digital technology, however, it has become difficult, if not impossible to trace and track the chain of infringement. Thus, there is a need for a more elaborate law to cover the existing gaps in regulation and make stricter regulations for online activities that relate to protected works.

IV. Digital rights and freedoms

[35] Gabsa, L. D. N. (2024). Copyright Infringement in the Information and Communication Technology (ICT) Era. Law and Humanities Quarterly Reviews, 3(1), 97-106.
[36] *Google LLC v. Oracle America*, Inc. (2021) 141 S. Ct. 1163.

Digital rights and freedom are extensions of fundamental rights granted to individuals by law. It means being entitled to, online, the right to which a person is ordinarily entitled. Rights such as the right against discrimination, right to privacy, freedom of information, freedom from violence, freedom of association, and freedom of expression are all exercisable rights both ordinarily and on the internet.[37] Presently, there is no specific legislation on digital rights but they are regulated by various laws, declarations, regulations, and international instruments. Being fundamental rights, digital rights are also regulated by the Universal Declaration of Human Rights, The Constitution of the Federal Republic of Nigeria, 1999 as amended and a host of other national and international laws with provisions for fundamental rights.

There are, however, some challenges with digital rights, the government seems to usually restrict digital rights especially as it relates to freedom of expression based on national security and public order. In addition, many jurisdictions lack comprehensive legal frameworks to address digital rights, leaving individuals vulnerable to exploitation. In addition, the likelihood of infringement of rights outside the internet is the same on the internet, internet bullies, discrimination, fake news, breach of privacy etc all happen on the internet, hence, the need for comprehensive legislation that clearly outlines the rights, duties, liabilities and obligations of all users of the internet whether individual, companies of government entities.

V. Artificial Intelligence

Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence, such as learning, problem-solving, and decision-making.[38]AI systems are designed to handle complex tasks by analysing data, recognizing patterns, and making decisions based on that analysis. These systems have the potential to revolutionize various industries, including healthcare, finance, and transportation.

One of the significant advantages of AI is its ability to increase efficiency and accuracy in various tasks. AI systems can automate repetitive and mundane tasks, freeing up

[37] Toyin Akinniyi, 'Digital Rights in Nigeria: Emerging Issues and Opportunities' https://www.luminategroup.com/posts/news/digital-rights-in-nigeria-emerging-issues-and-opportunities accessed 22 January 2025; African Digital Rights Network, 'What are Digital Rights' https://www.africandigitalrightsnetwork.org/what-are-digital-rights- accessed 22 January 2025.

[38] Kurzweil, R. (2005). The singularity is near: When humans transcend biology. Penguin.

human resources for more strategic and creative work.[39]Additionally, AI can analyse vast amounts of data quickly and accurately, reducing the likelihood of human error. This has significant implications for industries such as healthcare, where accurate diagnosis and treatment are critical.

However, AI also has its drawbacks. One of the significant concerns is job displacement, as AI systems automate jobs that were previously performed by humans.[40] This could exacerbate income inequality and lead to social unrest. Furthermore, AI systems can perpetuate existing biases and discriminate against certain groups, particularly if the data used to train AI systems is biased. This highlights the need for careful consideration of the data used to train AI systems and the need for transparency in AI decision-making processes.

Another significant concern is the potential security risks associated with AI. AI systems can be used to launch cyberattacks, steal sensitive data, and compromise national security.[41] This highlights the need for robust security measures to protect AI systems and prevent them from being used maliciously. Furthermore, there is a need for international cooperation to develop norms and standards for the development and deployment of AI systems.

In terms of real-world applications, AI is being used in various industries, including healthcare, finance, and transportation. For example, AI-powered chatbots are being used in customer service to provide quick and accurate responses to customer inquiries.[42] Additionally, AI-powered image recognition systems are being used in healthcare to analyse medical images and diagnose diseases.[43]

# 4. Legal and institutional framework on Digital Technologies in Nigeria

There are many and varied frameworks on digital technologies in Nigeria. They include the following:

[39] Davenport & Dyché, (2013). Big data in big companies. International Journal of Business Intelligence Research, 4(1), 1
[40]O'Neil, 2016. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.
[41] Kaplan, 2016 Artificial intelligence: What everyone needs to know. Oxford University Press.
[42] Huang, M. H., & Rust, R. T. (2017). Artificial intelligence in service. Journal of Service Research, 20(2), 155-172.
[43] Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., & Kearnes, K. (2017). Deep learning for healthcare: Review and applications. IEEE Journal of Biomedical and Health Informatics, 21(4), 821-833.

A. The Constitution of the Federal Republic of Nigeria, 1999

The Constitution of Nigeria serves as the foundational legal framework, conferring validity on all subsidiary laws and regulations governing record keeping in the country.[44] Section 1(1) of the 1999 Constitution establishes Nigeria as a sovereign state, predicated on democratic principles and social justice. This provision sets the tone for the protection of citizens' rights, including the right to privacy, which is fundamental to record-keeping practices.

Section 37 of the Constitution of the Federal Republic of Nigeria (1999) unequivocally guarantees and protects the privacy of Nigerian citizens, encompassing various aspects, including personal privacy, home privacy, and confidentiality of correspondence, telephone conversations, and telegraphic communications. This provision ensures that citizens' personal information and communications are shielded from unauthorized access or intrusion, except as permitted by law.

B. Nigerian Data Protection Act, 2023

In response to the call for a more robust data protection instrument to adequately provide for the collection and processing of data in Nigeria, the Nigerian Data Protection Act, 2023 was signed into law on 12 June 2023. The Act seeks to give proper regulation for the processing of data and the rights of data owners. Out of the numerous issues addressed in the Act is a veritably striking and applicable provision to the health sector and the processing of sensitive personal data. Section 24 of the act provides for the principles of personal data processing.

> "(1) A data controller or data processor shall ensure that personal data is —
> (a) processed in a fair, lawful and transparent manner;
> (b) collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;
> (c) adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;
> (d) retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed;
> (e) accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed; and
> (f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.

> (2) A data controller and data processor shall use appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data."

C. European General Data Protection Regulation 2018

General Data Protection Regulations (GDPR) is an EU law with obligatory rules on how organisations and companies must use particular data. Data must be used with integrity and in a friendly way, for example, information which can directly identify a person, such as name, phone number, home address and correspondence among others must be kept confidential.

Each Organization that processes particular data of workers and guests must ensure that the data being used fulfils the demand for which the data is collected. The use of a particular data must therefore be legal.

The use of data must not also contradict individuals' rights. The GDPR provides each person with certain rights to their particular data. They have the right to gain access to their particular data, rights to know how an organization is using the data, and object to the processing, etc.

The GDPR Personal data breaches must be reported within 72 hours. In the event of loss of sensitive data, similar to health or fiscal data, the incident must be reported to the authority within 72 hours. The regulation also imposes duties on the controller to contractually regulate that its suppliers follow the data protection regulations. If the controller should put data at threat the controller will be responsible. An organisation is expected to inform citizens and guests on data usage in a transparent manner. The individualities whose particular data you process (data subjects) must be informed of your processing. To this end, organisations use Notices and colourful programs on websites, as part of service agreements, and etcetera.

Furthermore, an organization is expected to assign a Data Protection Officer (DPO) to the organisation's work. The DPO should be reported to the responsible data protection authority in the country where the organisation is established.[45] For any business relationship, there is a need to have a Data Processing Agreement (DPA) in addition to the main agreement. A DPA sets out rules for how the Processor may use particular data to fulfil the purpose for which the data is collected.

[45] General Data Protection Regulation 2018, Article 37-39

The summary of the GDPR is that the law establishes scores for businesses and provides rights for citizens. Businesses are wise to modernise or establish their data protection compliance programme as the GDPR imposes sanctions on violators by putting substantial forfeitures for companies not following the rules. There is also a provision for Data Protection Impact Assessment (DPIA) which is set out in Section 35 of the GDPR.

D. Artificial Intelligence Act

The European Union Artificial Intelligence Act or the Artificial Intelligence Act is a law that governs the development and the usage of Ai in the European Union (EU). The Act regulates the use of Artificial Intelligence. The Act applies to multiple drivers in the AI value chain, similar to providers, deployers, importers, distributors, product manufacturers and authorized representatives).

The Act defines an AI system as a system that processes inputs and is autonomous. It defines GPAI as AI models that display significant generality, have the ability to perform a wide range of distinct tasks, which can be integrated into a variety of downstream AI systems or operations. For illustration, a foundation model is a GPAI; a chatbot or generative AI tool erected on that model would be an AI system.

The Act also applies to providers and deployers outside of the EU if their AI, or the services of the AI, are used in the EU. While the act has a broad reach, some uses of AI are exempted from liability, particularly uses of AI, and AI models for scientific exploration and development, are exempted from liability.

E. African Union Convention on Cyber Security and Personal Data Protection (2014)

This convention aims to promote cybersecurity and data protection in Africa, emphasizing the importance of cooperation and coordination among member states.[46] Despite the existence of these frameworks and laws, challenges persist in ensuring effective data protection. The rapid evolution of technology, cross-border data transfers, and the need for harmonization among different legal frameworks are some of the pressing issues. As data protection laws continue to evolve, it is essential for

[46] Perspective A Brief Introduction to the Right to Privacy – Ana Mishova; Data protection laws around the world ; A Global perspective available on https://gdprlocal.com/data-protection-laws-around the world-a-global-perspective retrieved on 28/01/2025

organizations to stay informed and adapt to these changes to ensure compliance and protect individuals' privacy rights.[47]

# 5. Conclusion

The paper has demonstrated the prevalence of digital technologies as it evolved from the days of ENIAC to the present day, when AI and chatbots have become popular. The paper also captured almost all spheres of businesses profession, social, economic and political lives. It is discovered that as digital technology develops, different laws in different jurisdiction has always been enacted to make provision for the regulation of such technologies. It is however, noted that laws and regulation seems to always have been insufficient to cover the large expanse of areas that technology has covered. This has been the situation when it comes to the regulation of digital technologies in the 21st century. Technologies such as Artificial Intelligence, crypto-currency, block-chain have generated causes for concern in the field of data privacy rights, intellectual property infringements, and the most contemporary issues of digital rights. The study hereby concludes that, although there are substantial legislations, enactments and regulations for the control of digital technology systems, these laws seems to lag behind and is not quickly catching up with the present day realities enough. Thus, it is recommended that proactive legislation should be promoted. Legislature should not wait until the negative effect of a particular digital system is prevalent before it is regulated, it is also recommended that, in the age of digital technologies, technology inclined individuals should be encouraged to be part of the law-making process and not mere members of some committees that make recommendations, this will help drive home the point on the importance of regulation and the effect if otherwise not regulated.

KBLSP Journal

[47]<https://www.bing.com/fd/ls/GLinkPing.aspx?IG=EC838E8D6E674EAA89C3B8FD40E9A174&&ID=SERP,5147.2&SUIH=N3ufFw-6c89U8FeHj7K6CQ&redir=aHR0cHM6Ly9kamlscC5vcmcvaW50ZXJuYXRpb25hbC1sZWdhbC1mcmFtZXdvcmtzLW9uLWN5YmVyc2VjdXJpdHktYW5kLWRhdGEtcHJvdGVjdGlvbi1sYXcv