IMPACT OF INFORMATION TECHNOLOGY ON CIVIL RIGHTS AND CRIMINAL LIABILITIES

Honesty Eguridu[1], Tybones Tolani[2], Oke Olusola[3], & Wilson Sakpere[4]

Abstract

This paper reviews the contemporary challenges of the impact of information technology on human rights and criminal liabilities. Technologies that once enhanced the fight against human rights abuses are now being weaponized by state and non-state actors to harass, survey, and track the activities of citizens and violate their rights. Moreso, the innovation of artificial intelligence (AI) entities in critical sectors of human endeavors has thrown up issues of human rights implications of algorithm-based decision making. AI entities have displayed tendencies of bias and tended to be incapable of fair decisions at all times. The question is how safe is it to delegate some human mental activities such as making of decision to AIs? Generally, criminal liability arises out of the presence of two factors: mens rea and actus reus. The challenge is whether AI is capable of forming mens rea. This paper evaluates various views on these challenges with the aim of finding solutions to how the rights of citizens can be better protected against application of new technologies by both state and non-state actors. We will also examine whether our current criminal laws can be applied to hold AIs liable for criminal offences and proffer solutions how AIs should be treated with regard to criminal liabilities. This paper recommends that the Turing Test should be applied to determine whether an AI has the capacity to develop guilty mind or mens in order to determine its criminal liability.

---

[1]LLB (Hons), LLM, Barrister at law and PhD Candidate, Lead City University, Ibadan; Email: honestyeguridu@yahoo.com

[2] LLB (Hons) LLM, Barrister at law and PhD Candidate, Lead City University, Ibadan. Email: tytbonestolani@gmail.com

[3]LLB (Hons), LLM, Barrister at law and PhD Candidate, Lead City University, Ibadan. Email: olusolaokelaw@gmail.com

[4]PhD, Lecturer and Head of Department, Computer Science, *Lead City University, Ibadan*

Keywords: Information Technology, Human Rights, Artificial Intelligence, Criminal liability

1.0 Introduction

The impact of information technology (IT) on the enjoyment of human rights and in criminal liabilities is almost unlimited. Information technology provides new avenues for advocacy, defense, and exercise of human rights across all types of rights, be it political or civil as well as social rights cultural, and economic rights. Information technology shapes how people access and share information, form their opinions, debate, and form associations. These have deeply transformed the "public square"[5]. But digital technology is often times abused to suppress, limit and violate rights, through processes like surveillance, censorship, online harassment, algorithmic bias and automated decision-making systems.

The abuse of digital technology also disproportionately affects marginalized individuals and groups, leading to inequality and sometimes this leads to discrimination, racial and gender biases - both online and offline. The use of information technology in each of these contexts does not simply pose risks to rights but more fundamentally poses risks to accountability. Humans are naturally endowed with intellect. The intelligence of man further propelled humans to create entities to enhance the abilities of man to do certain things with speed and precision that is ordinarily beyond human capacity. Computers and Artificial intelligences entities were therefore manufactured to enhance human intelligence but not to replace man in performance of some key human activities, especially activities that require human discretion and deep human reflection. However experience has shown that computers and intelligent machines are fast replacing human simple activities. Artificial intelligence is now involved with what man does every day in most human societies with its implications both positive and negative[6].However, the relevant question is whether an AI is capable of being held liable for crimes committed out of its own volition. Can a non-human entity be held liable to have guilty mind within the existing

[5] United Nations Human Rights office of the High Commissioner: Digital Space and Human Rights. Available at https://www.ohchr.org/en/topic/digital-space-and-human-rights (accessed on 3 October 2023)

[6]Molly K. Land[1] and Jay D. Aronson, Human Rights and Technology: New Challenges for Justice and Accountability. Available at https://doi.org/10.1146/annurev-lawsocsci-060220-081955 accessed on 12 October 2023

laws and principles in our criminal law jurisprudence? Is it possible to hold a machine liable *vis-a-vis* the well-entrenched principles criminal law?

This paper will examine ways information technology has relegated human rights and how the negative trend can be addressed and how duty bearers and violators of human rights can be held accountable. The paper will also examine some of the proposition made by scholars to resolve the issue of criminal liability when an Artificial Intelligence entity is involved in a crime. The paper will also consider the criminal liabilities of various actors in the chain of interaction in the use of the cyberspace that leads to violation of human rights and or criminal offences. The views of scholars will be outlined with special focus on current position of the law in Nigerian and laws of other jurisdictions with a view to ascertain if the laws as currently constituted can address the seeming gap between the traditional mode of determining and apportioning responsibilities and liabilities and challenges being thrown up by new trends of technology. This paper will also advocate the use of Turing Test in determining whether robots or computers can be held liable when human rights are violated and whether they have the ability to develop guilty minds.

2.0 The Concepts of Human Rights and Criminal Liability in Perspective

According to the Equality and Human Rights Commission[7], Human rights are the basic rights and freedoms that belong to every person in the world, from birth until death. These rights apply regardless of where the individual is from, what the individual believes or how such person chooses to live. These rights can never be taken away, although they can sometimes be restricted – for example if a person breaks the law, or in the interests of national security. These basic rights are based on shared values like dignity, fairness, equality, respect and independence. These values are defined and protected by law[8]. In Nigeria, for example, human rights are protected by Chapter four of the 1999 Constitution while in Britain human rights are protected by the Human Rights Act 1998.

Criminal liability on the other hand, is the liability to be punished in a criminal proceeding. In criminal liability, punishment is awarded to a

[7] https://www.equalityhumanrights.com/human-rights/what-are-human-rights

[8] Equality and Human Rights Commission> Available at What are human rights? | Equality and Human Rights Commission (equalityhumanrights.com)

wrongdoer. If the person is guilty of committing the offense with criminal intention then he is liable for punishment. Criminal liability is based on the Maxim "*actus non facit reum nisi mens sit rea*" it means the offender is guilty only when it is done with the guilty mind[9].

3.0 Civil Rights Abuses and Criminal Liabilities Associated with Digital Technology Innovations

To be considered here are three developments in the field of technology and human rights that have become increasingly of concern over the past decade. These are: government surveillance and harassment, the role of AI in the context of automated decision-making and deep fakes, and the rise of the digital state.

3.1 State Surveillance and Harassment

The time of technology as a potential disruptor of state power is long past[10]. Today, technology more often serves to reinforce and consolidate state power[11]. Executive Directors of the nongovernmental organization witness, technologies like mobile phones and social media, once touted as liberating, have largely been co-opted by state actors.[12] Governments and state-aligned actors use extraordinarily powerful spyware and other new tools to control and manage the information space and thereby constrain activists, journalists, and other civil society actors.[13] These tools fall into two categories: tools of harassment and tools of surveillance[14].

3.2 Harassment

Celebrity actors are increasingly using tools such as social media to attack and undermine their opponents[15]. Attacks on human rights defenders, coordinated on social media, not only have a chilling effect on the activities of individual defenders but also undermine public support for their

---

[9]SRD law notes. Available at What is Liability and what are Different Kinds/ Types of Liability - SRD Law Notes (accessed on 19 October 2023)

[10] ibid

[11] ibid

[12] Gregory S. 2019. Cameras everywhere revisited: how digital technologies and social media aid and inhibit human rights documentation and advocacy. *J. Hum. Rights Pract.* 11(2):373–92

[13] ibid

[14]Molly K. Land[1] and Jay D. Aronson, op cit

[15]ibid

activities.[16] State actors actively seek to discredit content produced by citizens and activists through trolling or disinformation campaigns or through threats to their well being.[17]

Governments are now diverting the strengths of social media against activists.[18] It has been said that government propagandists often exploit distributed architecture and low gate keeping, which enable online organizing, to discredit opposing sources of information[19]. Revolutions depend on activists' ability to convey credible information. In the current trend of fake news and troll farms, it is difficult to know what to believe, even for those with the resources to inquire.[20]

Government authorities in the world over use disinformation and misinformation to undermine dissenting views and criticisms, restrict the space for civil society organizations, and even in some instances incite violence.[21]. Disinformation may increasingly take the form of fake audio or video generated by AI systems that use old video to synthesize entirely new content that has no basis in reality.[22] Several scholars have written about threats posed by deep fakes, including a range of harms both to individuals and to society as a whole[23]. These deepfakes are often used to conduct credibility attacks, to muddy the waters of investigations, and to incite violence against journalists and human rights defenders."[24]

---

[16]ibid

[17] Gregory S. 2019, op cit

[18]Tufekci Z. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, CT: Yale Univ. Press

[19] ibid

[20] ibid

[21]Kelly S, Truong M, Shahbaz A, Earp M, White J. 2017. *Freedom on the net 2017: manipulating social media to undermine democracy*. Doc., Freedom House, Washington, DC. Available at https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy(Accessed on 13 October 2023

[22] ibid

[23]Chesney B, Citron D. 2019. Deep fakes: a looming challenge for privacy, democracy, and national security. *Calif. Law. Rev.* 107:1753–819

[24]Gregory S. 2019, op cit, p. 380

3.3 Surveillance

States are also using surveillance tools to maintain and consolidate power. As documented by Amnesty International in a report[25], government in Morocco used a certain Pegasus spyware, produced by an Israeli firm called the NSO Group This software is able to monitor and possibly attack defenders of human rights.[26]When the software is installed on a phone, it can extract all of the data on the device, including text messages, contacts, GPS location, email and also browser history. It can additionally create new data by using the phone's microphone and camera to record the user's surroundings and ambient sounds[27]

AI, cloud computing, and the lack of a privacy-protecting legal framework enable this surveillance to take place 24 hours a day, 7 days a week throughout almost all public and private spaces in many countries.[28] Many states further support their surveillance efforts by limiting access to encryption technologies, banning VPNs (virtual private networks) that can obscure the identity and location of Internet users, and threatening those who record state actors in public with physical violence or criminal action[29]. These efforts constitute a weaponization by states of what activists had initially hoped would be tools of "surveillance," or counter forensics[30],In the context of surveillance, spyware such as Pegasus is created and sold by

---

[25] Amnesty International. 2019. Morocco: human rights defenders targeted with NSO group's spyware. *Amnesty International*, Oct. 10. Available at https:// www.amnesty.org/en/latest/news/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/Accessed on 15 October 2023

[26]Amnesty International. 2019. Morocco: human rights defenders targeted with NSO group's spyware. *Amnesty International*, Oct. 10. Available at https://www. amnesty.org/en/latest/news/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/(Accessed on 15 October 2023)

[27]Hopkins N, Sabbagh D. 2019. WhatsApp spyware attack was attempt to hack human rights data, says lawyer. *Guardian*, May 14. .Available at https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperateAccessed on 17 October 2023

[28] ibid

[29]Kelly S, Truong M, Shahbaz A, Earp M, White J. 2017, op cit

[30]Weizman E. 2017. *Forensic Architecture: Violence at the Threshold of Detectability*. Brooklyn, NY: Zone Books

private companies.[31]All these instances are flagrant violation of the rights of citizens to privacy.[32]

4.0 Artificial Intelligence and Automation

Over the past decade, the human rights implications of algorithm-based decision making have become increasingly concerning[33]. The AI Now Institute defines automated decision systems as "data-driven technologies used to automate human-centered procedures, practices, or policies for the purpose of predicting, identifying, detecting, and targeting individuals or communities"[34]. These technologies are used in a wide variety of contexts, including "to allocate finite government resources (e.g., public benefits or health services); to foresee and presumably prevent specific risks or adverse outcomes; to remove or curtail discretion from current human decision-making; and to provide analysis at a scale and scope that cannot be performed by humans"[35]

Algorithms are opinions embedded in codes. Recent studies around bail, sentencing, policing, and parole from the criminal justice system have received a great deal of attention[36] and have exposed the potential negative

---

[31]Molly K. Land[1] and Jay D. Aronson, op cit

[32]spyware. *Amnesty International*, Oct. 10. Available at https://www.amnesty.org/en/latest/news/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/(Accessed on 15 October 2023) see also Abbas M, Al-Wohaibi E, Donovan J, Hale E, Marugg T, et al. 2019

[33]Angwin J, Larson J. 2016b. Bias in criminal risk scores is mathematically inevitable, researchers say. *ProPublica*, Dec. 30. .Available at https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say(Accessed on 16 October2023)

[34] Richardson R, Cahn A, Kak A, Diaz A, Samant A, et al. 2019a. *Confronting black boxes: a shadow report of the New York City Automated Decision System Task Force*. Rep., AI Now Inst., New York. Available at https://ainowinstitute.org/ads-shadowreport-2019.pdf (Accessed on 18 October 2023)

[35] ibid

[36] Barry-Jester AM. 2015. Should prison sentences be based on crimes that haven't been committed yet? *Five Thirty Eight*, Aug. 4. Available at https://fivethirtyeight.com/features/prison-reform-risk-assessment/(Accessed on 3 October 2023); Chammah M, Hansen M. 2016. Policing the future. *The Marshall Project*, Feb. 3. Available at https://www.themarshall project.org/2016/02 /03/ pol icing-the-future(Accessed on 14 October 2023); Corbett-Davies S, Pierson E, Feller A, Goel S. 2016. A computer program used for bail and sentencing decisions was labeledbiased against blacks. It's actually not that clear. *Washington Post*, Oct. 17. Available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/

aspects of AI in hiring decisions and workplace affairs[37],[38] and health care[39]. There has also been significant concern about the human rights implications of AI in facial recognition systems,[40] weapons systems, autonomous vehicles, and elsewhere.[41]

4.1 Wrong Use of Deepfake Technology Associated with AI

Deepfakes technology involves the use of advanced artificial intelligence methods such as deep learning algorithms to create realistic yet misleading content. This craft, which has its good side for its entertainment value, can be achieved by overlaying a person's face into another person's body in order to deceive the viewing public to believe that the person in the video is involved in an act or made a statement that never happened. As deepfake technology continues to evolve, ethical guidelines and regulatory measures are needed to address the risks and consequences associated with digital media manipulation[42]. The advent of deep fake technology has given rise to new concerns about digital manipulation and calls for vigilance and proactive measures to maintain the integrity of online information and interaction. It is pertinent to note that in Nigeria there is currently no law prohibiting the use of deepfake for negative purposes. The applicable laws only makes provisions against fraudulent contents, harassment, defamation, and copyright infringement, as well as data protection regulations. So if

---

10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/(Accessed on 14 October 2023)

[37]Bolukbasi T, Chang K-W, Zou J, Saligrama V, Kalai A. 2016. Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. In *Proceedings of the 30th Conference on Neural Information Processing Systems (NIPS 2016)*, pp. 4356–64. New York: Assoc. Comput. Mach.;

[38] Dattner B, Chamorro-Premuzic T, Buchband R, Schettler L. 2019. The legal and ethical implications of using AI in hiring. *Harvard Business Review*, April 25. Available at https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring Accesses on 17 October 2023

[39] Obermeyer Z, Powers B, Vogeli C, Mullainathan S. 2019. Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 366(6464):447–53

[40]Garvie C, Bedoya A, Frankle J. 2016. *The perpetual line-up: unregulated police face recognition in America*. Rep., Georgetown Law Cent. Priv. Technol., Washington, DC. Available at https://www.perpetuallineup.org/(Accessed on 6 October 2023)

[41]Molly K. Land[1] and Jay D. Aronson, op cit

[42]See https://www.thomsonreuters.com/en-us/posts/technology/practice-inno va tions-deepfakes/ Accessed on 13November 2023

someone's rights are harmed by deep fakes there are no legislation to seek redress under the criminal law against such contents in Nigeria. The case is different in China's and some states in US where the use of deep fakes are criminalized in some specific instances[43]. There is therefore an urgent need to amend the Cybercrimes (Prohibition and Prevention) Act, 2015 to make specific provisions to criminalize use of deep fakes for negative or harmful purposes.

5.0 The Notion of Criminal Liability

The question of liability is central in the essence of criminal law jurisprudence globally. The germane question is whether an entity be it human or corporation is criminally liable with regard to a particular offence committed at a given time and space.[44] A perusal of criminal law legislations in Nigeria, especially sections22–36,in chapter 5 of the Criminal Code Act, dwell on criminal liability.

The Criminal Code provides in Section30that everyone below seven years is exempted liability for crimes with regard to any act or omission. The Act also exempts persons below twelve years of age from criminal liability whatsoever. The exception is that if it can be established that at the time of carrying out the act or omission the child had the capacity to understand that he ought not to carry out such act or omission.Section28 of the Act also provides that a person is not criminally responsible if at the time of carrying out an act or omission he is not is a state of mind or metal orientation to understand that he ought not to carry out such act or omission either as a result of mental disease or infirmity he is deprived of forming the ability to control or understand his action or omission.

Criminal Code Act in Section 7 provides for parties to offences in the following manner-

The following persons are deemed to have taken part in committing an offence whenever an offence is committed ;

(a) Everyone who actually does the act or makes the omission which constitutes the said offence;

(b) Everyone who does anything or omit to do anything that aids another in committing the offence

(c)Everyone who actually aid another person in committing the offence.

---

[43] ibid

[44]Ikenga K.E. ORAEGBUNAM, and Eme UGURU,. Artificial Intelligence Entities and Criminal Liability: A Nigerian Jurisprudential Diagnosis: Available at - Academia.edu (Accessed on 10 October 2023)

(d)Anyone who counsel another person or procures the person to commit the offence

The universally acceptable elements of liability for criminal action now forms part of Nigerian criminal law jurisprudence. The maxim in Latin is "*actus non facit reum nisi mens sit rea*", which can be interpreted in English as "an act does not make a person guilty unless there is a guilty mind" The two elements used in determining criminal liability in criminal law jurisprudence today evolved from this maxim. These are *Actus Reus*(the wrong act) and *Mens Rea* (the mind that is guilty).[45]The general principle of law is that if one of these two elements is missing in a criminal act or omission, there cannot be criminal liability. The same principle applies to humans, corporations or Artificial Intelligence entities.[46]

The point must also be made that for there to be a criminal liability the person or persons involved in the act must be recognized by law as a person. And such a person must not have been excluded from criminal liability or culpability by any law and the act or omission must be backed by the knowledge of crime. Gabriel Hallevy advocated the imposition of criminal liability on Artificial Intelligence entities using three possible models of liability: These are: Perpetration – via –Another liability model; the Natural-Probable-Consequence liability model; and the direct liability model[47]The Perpetration-via-Another liability model do not view AI as having the ability to possess any human attributes.[48]The AI is viewed here as an innocent agent.[49]According to this model, machine can never be hum and has no ability to be held guilty. The point must be made that the proponents of this model acknowledge the abilities of an Artificial Intelligence entity's to carry out many actions but they argued that these abilities can never be grounds to consider an AI as having the abilities to commit a crime.[50]

---

[45]Hallevy, Gabriel (2010) "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control," Akron Intellectual Property Journal: Vol. 4 :Iss. 2 , Article 1. Available at: https://ideaexchange. uakron.edu/akr onint el lectualproperty/vol4/iss2/1 (Accssed on 19 October 2023)

[46]Ikenga K.E. ORAEGBUNAM, and Eme UGURU, op cit

[47] ibid

[48] ibid

[49] ibid

[50] ibid

The relevant question with regard to AIs is: Who can be held liable as the perpetrator-via-another when an AI commits an offence?[51] The proponents of this model has posited that there are two categories of persons, they are: the person who programmed the AI software and the end user[52] Legally, in the both scenarios, it is only the AI that the offence can be attributed to because the actus reus cannot be ascribed to the person who programmed or the end user . So none of the two instances satisfy the *actus reus* required to impute guilt in the particular offence.[53]

The second model is the Natural-Probable-Consequence liability model which is applicable when the programmers or end users are deeply part of the daily activities of the AI but with no intention on their part to use the AI to commit an offence.[54]This model is applicable if the AI in its daily tasks commits an offence without the knowledge or intention of the programmer or user, which act is discovered after the offence has been committed. This model applies the foreseeability test. Is it foreseeable for the person who programmed the AI software or end users to know that the AI has the capacity or propensity to commit the offence?[55] This model is of the view that anyone can be liable if the offence is foreseeable or probable consequence of the person's action.[56]It is pertinent to point out that the natural-probable-consequence liability model is applicable in two distinct scenarios[57]. The first is whether there is negligence on the part of the programmer or end user but without intention on their part to commit a crime.[58]. The second scenario is whether the person who programmed or end user intentionally set out to commit an offence with the AI, but it turns out that the AI failed to follow the plan and committed a different type of offence instead of or in addition to the intended offence.[59]The first scenario is rooted in negligence per se which can incur criminal liability.[60]. The second scenario clearly evinces the programmer's or end user's culpability as they can be held liable for both the offence intended to be committed via the AI and the ancillary

[51] ibid
[52] ibid
[53] ibid
[54] ibid
[55] ibid
[56] ibid
[57] ibid
[58] ibid
[59] ibid
[60] ibid

offence committed in the process or the offence committed instead of the planned offence.[61]

The third model is the direct liability model of AI. This model is purely focused on the Ai itself. It is not concerned about the person who programmed the software or end user of the AI.[62] It is based on the premise that if an AI fulfills the requirements of the two elements of mens rea and actus reus then the AIis capable of being held criminally liable.[63] The objective question is why should an entity that satisfies the requirements of criminal culpability be exempted from liability?[64]This is the crux of the strong point advanced by the direct liability model. It has been proposed, and we align with this view, that to be held liable for crime, AIs must be clothed with legal personality as in the case of corporations which are addressed in the garb of corporate legal personality.[65] AIs should likewise be accorded such statutory legal personality. This proposition is apt because AIs has the capabilities to carry out action of their own volition and they have the ability to develop and think for them and can take decisions that can give rise to criminal and civil liabilities alike.

6.0 Artificial Intelligence Entities and Liability for Crimes in Nigeria

Nigerian laws used the word 'person(s)'to define offences and to ascribe punishments. The Nigerian constitution inSection36 (12) used the word 'person' to enshrine an important elements that must be satisfied for anyone to be held accountable for a criminal offence. The above mentioned constitutional provision makes it a condition precedent that before a criminal offence can be imputed to anyone, the identity of that person must be certain. The person must be a proper person recognized by law[66]In this vein, it is important to point out that AIs not recognized or mentioned in any legislation in Nigeria as having a legal personality.[67]

It has been argued that it is impossible to ignore granting AI legal personality because they are increasingly being involved in human daily activities in the

---

[61] ibid

[62] ibid

[63] ibid

[64] ibid

[65]Ikenga K.E. ORAEGBUNAM, and Eme UGURU, op cit

[66] ibid

[67] ibid

form of humans[68]AIs endowed with intelligence and are able to take their own decisions, learn from past experience, memorize, strategize, show complexity, and capacity to manipulate structures and thus behave like humans.[69]. With the present state of Nigerian law as enshrined in section 36 (12) of the constitution, AIs are not recognized as persons to qualify them for criminal liability for crimes committed by them. The recommendation therefore is that for AIs to be held liable for crimes, new and existing criminal law legislations must make specific provisions on AI's liability.[70]

The applicability of sections 28 and30 of the Criminal Code to AIs is that since AIs are not recognized as persons they cannot be said to have mental capacity to commit any crime. So AI.s will be exempted from criminal liability under the criminal code for lack of mental capacity.[71]There is therefore an urgent need for legislative reform on AIs' activities in Nigeria.

7.0 Conclusion and Recommendations

Nigeria is a major hub of the global cyberspace community. The figures have shown that about 55.4 percent of Nigerian population put approximately at 122.5 million people use the internet daily as at January 2023[72]. The steady growth in the number of Nigerians using the internet and invariably exposed to digital technology over the years is a good development but it also call for concern about how this huge population of internet and digital technology users are regulated. Lack of a strong legal regime to tackle the new challenges associated with the cyberspace often bring about abuse of human rights and lack of accountability in holding offenders liable for crimes perpetrated through the cyberspace and use of digital technology.

Digital technology is breaking new grounds and throwing up new challenges and the law cannot be lagging behind in catching up with the new reality. The law therefore must be made to come in terms with new realities such as deepfake technology and artificial intelligence. Abuse of human rights through surveillance and breach of the rights to privacy must also be checked. The court must rise up to the occasion to hold government and

---

[68]Paulius C˘ erka, Jurgita Grigiene˙,Gintare˙Sirbikyte (n.6) p. 685–699

[69]ibid

[70] ibid

[71] ibid

[72]See https://datareportal.com/reports/digital-2023-nigeria#:~:text= There%20were%20122.5%20million%20internet%20users%20in%20Nigeria%20in%20January,percent)%20between%202022%20and%202023. Accessed on 30th October 2023

private individuals who violate these rights accountable. The court must ensure that duty bearers and anyone who violates the rights of citizens through the cyberspace must be held accountable with the existing provisions of the Constitution on fundamental rights.

New laws must also be enacted with urgency to provide for the use of new technologies such as deepfake and artificial intelligence. AI entities must be clothed with legal personality to make them liable for crimes committed by their own volition. The law must ensure that innovators are only held accountable for crimes caused by criminal negligence and those they intentionally cause AIs to commit. This way, innovators will not be scared away from making inventions.