journals.unizik.edu.ng/jcpl/index ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW Vol. 12(3), July, 2025

JUDICIAL PERSPECTIVES ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE: A REVIEW OF DECIDED CASES

Gladys Uzoamaka Eze*
Peace Udoka Ogbonna**

Abstract
Artificial Intelligence is transforming various aspects of human life. The evolution of Artificial Intelligence creates concerns over abuse of human rights and opportunities for human rights to thrive. The impact of artificial intelligence on human rights has not enjoyed judicial attention in the Nigeria. There is therefore the need to consider whether judicial interpretation of constitutional provisions guaranteeing rights, are sufficient to protect human rights which are impacted by Artificial Intelligence as it evolves. This study undertakes a critical review of judicial perspectives on the intersection of human rights and artificial intelligence in Nigeria. The study is purely doctrinal in nature, and employed the use of both primary and secondary sources of law in identifying and explaining the themes of this analysis. The study finds that while there are no specific actions affording the courts the opportunity to analyse the impact of artificial intelligence on human rights, the Courts have interpreted the law on integral aspects of Artificial Intelligence in its interaction with human rights, which will form a background for the development of effective programs and policies for the protection of rights in the face of Artificial Intelligence. The study recommends the utilization of Artificial Intelligence for the protection of human rights and the progressive interpretation of constitutional provisions to provide ample protection for human rights in the face of Artificial Intelligence.

Keywords: Artificial Intelligence, Human Rights, Judicial Perspectives.

1. Introduction

Artificial Intelligence has not enjoyed judicial consideration in Nigeria. However, certain Courts have made pronouncements on certain aspects of the constituents and working of Artificial Intelligence especially data privacy and cybercrimes. International judicial considerations of the effect of artificial intelligence on human rights have also been made to an extent which may act as a catalyst for the development of the Nigerian jurisprudence on the subject. The foremost judicial considerations of the elements of artificial intelligence especially as regards their interactions with human rights in Nigeria thus need to be reviewed to appreciate the expanding judicial status of human rights at present, in the light of evolving artificial intelligence.

2. The Intersection of Artificial Intelligence and Human Rights

Artificial Intelligence reshapes industries while raising pressing human rights concerns. AI-driven automation enhances efficiency but risks privacy breaches, algorithmic bias, and misinformation. Courts worldwide are tackling AI-related cases, reinforcing legal protections for data privacy and digital rights. AI's role in cybersecurity, surveillance, and content moderation impacts freedoms of speech and expression. Judicial interpretations, such as Nigeria's rulings on data protection, expand human rights discourse to include Artificial Intelligence governance. As Artificial Intelligence continues to evolve, regulatory frameworks must ensure ethical deployment, balancing technological advancements with fundamental rights, fostering fairness, accountability, and justice in a rapidly digitizing world.

While Artificial Intelligence accentuates the enjoyment of human rights, the pervasive nature of Artificial Intelligence technologies raises significant questions about how these rights are protected or compromised.[1] Right to privacy especially, data privacy is the most regularly impacted human rights in

***Gladys Uzoamaka Eze,** Professor, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra-State, Nigeria. 234-37429390.
****Peace Udoka Ogbonna,** PhD Candidate, Faculty of Law, Nnamdi Azikiwe University, Awka
[1] A Willie, 'AI and Human Rights: Examining the Intersection of AI Technologies with Fundamental Rights, such as Freedom of Expression and the Right to Privacy' (2024) < https://www.researchgate.net/publication/ 387364266_AI_and_Human_

the digital age. Artificial Intelligence could be applied in the detection of potential data breaches,[2]minimizing risk of data privacy breaches by automating digital processes,[3]improve privacy in digital and personal interactions, and data anonymization to protect users' identities while allowing data to be useful for analysis. Conversely, the right to privacy, especially data privacy when it interacts with artificial intelligence suffers varying risks including data exploitation where data is over-collected and insecurely stored,[4]unauthorized web monitoring, unauthorized location tracking,[5] and loss of autonomy over personal data. There are also increasing incidents of forced data submissions in the form of mandatory 'accept cookies' prompts, for access to goods and services digitally. These practices increasingly undermine the right to privacy of individuals where Artificial Intelligence technologies are deployed.

Artificial Intelligence significantly impacts the human right to work in both positive and negative dimensions. Artificial Intelligence may increase labour productivity by automating routine or unsafe tasks, and creating opportunities for upskilling, but also rapidly eliminate various job roles and cause unemployment.[6] Artificial Intelligence also has varying effects on the rights of workers in the workplace, opening them to unauthorized surveillance and reduced autonomy.

The right to education enjoys certain advantages by the deployment of Artificial Intelligence. Access to education is improved with the provision of digital education mechanisms, personalized learning tailored to individual needs, *etcetera.* However, these are not without the attendant drawbacks such as the diminution of human cognitive capacity by over-reliance on Artificial Intelligence mechanisms such as chat boxes and other AI models, dehumanized learning experiences,[7] and bias in grading or errors in instruction data where the Artificial Intelligence model deployed is trained on biased or erroneous data.[8]

For the right to health, which is like many human rights, directly linked to the right to life,[9] the risks and opportunities for the realization of the right to health and healthcare are related to the design, development and deployment of Artificial Intelligence technologies.[10] The use of Artificial Intelligence models improve diagnostics,[11]monitor and manage disease outbreak, and expand frontiers for the prevention and cure of diseases, thereby greatly optimizing the enjoyment of the right to health. Conversely, the deployment of Artificial Intelligence technologies may exacerbate biases, and open individuals to AI-powered errors in diagnostics and treatment of diseases. Access to justice for harms perpetrated using Artificial Intelligence models and mechanisms is also a rising issue, as the deployment of Artificial

Rights_Exploring_the_Impact_of_AI_Tech
nologies_on_Fundamental_Rights_such_as_Privacy_Freedom_of_Expression_and_Equality> accessed 31 May 2025

[2] C Goodman, 'AI in Cybersecurity: Transforming Threat Detection and Prevention' (2025) <https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/> accessed 2 March 2025

[3] B Gubitosa, 'How AI Is Improving Data Management' (2024) <https://rivery.io/data-learning-center/ai-data- management/> accessed 2 March 2025

[4] E Barnes, 'Why should data mongering be regulated?' (2024) <https://www.vktr.com/ai-upskilling/data- mongering-is-the-silent-ai-threat-to-privacy-and-personal-autonomy/> Accessed 27/2/2025

[5] A Granados, 'AI and Personal Data: Balancing Convenience and Privacy Risks' (2024) <https://velaro.com/blog/the-privacy-paradox-of-ai-emerging-challenges-on-personal
data#:~:text=Web%20Activity%20Monitoring%3A%20AI%20algorithms,it%20also%20poses%20privacy%20issues.> accessed 27 February 2025

[6] R Rodrigues, 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities' Journal of Responsible Technology [2020] (4) 100005, pp 5-6

[7] T B Fitria, 'Artificial Intelligence (AI) In Education: Using AI Tools for Teaching and Learning Process' (2021) https://www.researchgate.net/publication/357447234_Artificial_Intelligence_AI_In_Education_Using_AI_Tools_f
or_Teaching_and_Learning_Process/citation/download accessed 29/3/2025

[8] S V Chinta, Z Wang, Z Yin, N Hoang, M Nhat, M Gonzalez, T Le Quy & W Zhang, 'Navigating Fairness, Bias, and Ethics in Educational AI Applications' (2024) [7][27]

[9] H Nyane, 'The Interface Between the Right to Life and the Right to Health in Lesotho: Can the Right to Health Be Enforced through the Right to Life?' African Human Rights Law Journal [2022] (22) p 274

[10] I Ogunleye, L Tekisalp & H Darnton, 'The Role of AI in Healthcare' (2023) < https://www.bsr.org/reports/BSR- AI-Human-Rights-Healthcare.pdf> accessed 1/4/2025

[11] Spectral AI, 'Artificial Intelligence in Medical Diagnosis: How Medical Diagnostics are Improving through AI' (2024) < https://www.spectral-ai.com/blog/artificial-intelligence-in-medical-diagnosis-how-medical-diagnostics- are-improving-through-ai/> accessed 1/4/2025

Intelligence raises issues in liability and accountability.
The deployment of Artificial Intelligence enhances freedom of expression and access to information. Its use can empower voices of marginalized groups and improve access to information. Unfortunately, artificial intelligence has also been used as a tool to censor speech in digital spaces,[12] misinform, and circumvent the rule of law.

The interaction of Artificial Intelligence with human rights raises critical questions. While benefits are promised by the deployment of Artificial Intelligence in day-to-day human life, pressing challenges may also arise that undermine the enjoyment of rights. These include risks of algorithmic bias, invasive surveillance, loss of personal autonomy, and deepening inequalities. Ultimately, as Artificial Intelligence reshapes society, establishing robust ethical frameworks and regulatory safeguards is essential to ensure that technological advancements uphold human dignity and freedoms.

3. Judicial Approaches to Artificial Intelligence Related Cases on Human Rights

In today's rapidly evolving digital landscape, courts are increasingly called upon to navigate the complex interplay between artificial intelligence and human rights. Judicial approaches to AI- related cases must balance the promise of technological advancement with the need to protect fundamental freedoms such as privacy, equality, and due process. Artificial Intelligence is growing in its framework, and its elements have thus enjoyed only spare judicial considerations. However, certain Courts have made pronouncements on certain aspects of the constituents and working of Artificial Intelligence especially data privacy and cybercrimes that are pertinent in understanding the interpretation of existing laws for the regulation of these novel subject matters. As legal systems grapple with new challenges from algorithmic bias to data privacy breaches, this discourse examines how judiciaries are adapting legal frameworks to both harness innovation and safeguard human dignity.

3.1 Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC[13]

The facts of the case as presented by the Appellant before the trial Court was centered on an error in his National Identification Number Slip, which incorrectly stated his month of birth. Upon requesting a correction from the National Identity Management Commission, the respondent (NIMC) demanded a fee of N15, 000, citing its official policy and procedure. The appellant contested this requirement, arguing that it infringed upon his fundamental right to privacy and family life, as guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999. The Appellants as applicants by an Originating Summons and other accompanying processes all dated 12th February, 2020 sought from the trial Court the determination of the following questions:

a. Whether or not by the construction of Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended), the Respondent's act of demanding for payment for rectification/correction of personal data is likely to interfere with the Applicant's right to private and family life?
b. Whether or not by the provisions of Article 3:1(1) (7)(h) of the Nigeria Data Protection Regulation, 2019 (NDPR), the Applicants can request for rectification/correction of personal data from the Respondent free of charge.

Based on the determination of the above questions, the Appellants (Applicants) then sought for the following reliefs among others:

a. A declaration that demand for payment for rectification/correction of personal data of the Applicants is likely to violate the Applicant's fundamental rights to private and family life guaranteed under Section 37 of Constitution of the Federal Republic of Nigeria 1999 (as amended) and Article 3.1(1)(7)(h) of the Nigeria Data Protection Regulations, 2019 (NDPR).
b. A declaration that rectification/correction of personal data of the Applicants by the Respondent ought to be done without payment by virtue of Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and Article 3.1(1)(7)(h) of the National Data Protection

[12] D L Hudson, 'Chilling Effect Overview'(2020) < https://www.thefire.org/research-learn/chilling-effect- overview#:~:text= The%20%22chilling%20effect%22%20refers%20to,too%20broad%20or%20too%20vague,> accessed 11 April 2025
[13] (2021) LPELR-55623(CA)

Regulations, 2019 (NDPR).

The respondents' preliminary objection led to the suit being struck out, leaving the core issues unresolved. This prompted the appellant to file an appeal. The objection contested the court's jurisdiction, citing a lack of cause of action and arguing that section 37 of the Constitution did not safeguard data privacy. The Court of Appeal ultimately dismissed the appeal, deeming it lacking in merit. Consequently, the High Court of Ogun State's decision, delivered by Honourable Justice A. A. Akinyemi on July 15, 2020, which struck out the appellant's suit, was upheld.

It is however pertinent to note that of the issues submitted to the Court of Appeal for determination, Issue 2 on whether or not the trial Court was right when it held that the Appellants' suit which bordered on data protection did not disclose a cause of action under section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and thereby occasioned a miscarriage of justice to the Appellants, was considered and resolved. The Court in resolving this issue held as follows:

> *It is glaring that the phrase "Privacy of Citizens" is general and is not limited to any aspect of the person or life of a citizen. It is not expressly defined by the Constitution and there is nothing in the Constitution or any other statute from which it's exact meaning or scope can be gleaned.*

Further held by the Court in determining whether a cause of action on the infringement of privacy rights under section 37 of the Constitution had reasonably risen, was the dictum as follows:
In highlighting the absence of a clear scope of the right to "privacy of citizens" as guaranteed under Section 37 of CFRN, 1999, this Court, per Agim, JCA (as he then was, now JSC), had held in the cited case of NWALI v EBSIEC (2014) LPELR-23682(CA) at pages 27 - 29, para. E, as follows:

> *The meaning of the term "privacy of citizens" is not directly obvious on its face. It is obviously very wide as it does not define the specific aspects of the privacy of citizens it protects. A citizen is ordinarily a human being constitution of his body, his life, his person, thought, conscience, belief, decisions (including his plans and choices), desires, his health, his relationships, character, possessions, family, etc. So how the term "privacy of citizens" should be understood? Should it be understood to exclude the privacy of some parts of his life? This can be seen from its holding that the right includes "privacy in private family life and incidental matters when this aspect is not expressly provided for in that Section and that meaning is not patently obvious from the text of that Section...The privacy of home, privacy of correspondence, privacy of telephone conversations and privacy of telegraphic communication are clear and particular as to the nature of privacy protected or the area or activity in respect of which a person is entitled to enjoy privacy... It is glaring that the phrase "Privacy of Citizens" is general and is not limited to any aspect of the person or life of a citizen. It is not expressly defined by the Constitution and there is nothing in the Constitution or any other statute from which it's exact meaning or scope can be gleaned. (underline mine for emphasis)*
> *As observed above by His Lordship Agim, JCA (as he then was), the privacy of the home, correspondence, telephone and telegraphic communications protected by the Section are clearly definable and determinable as to their nature and scope. But the meaning and scope of "privacy of citizens" as guaranteed by the Section has not received clear definition/interpretation in the Constitution. The trial Court had, in my view, rightly held above, that the right to "privacy of citizens" as guaranteed under the Section includes the right to protection of personal information and personal data." Per MOHAMMED , J.C.A*[14]

Bearing in mind that by the provisions of the Constitution as well as Article 2(9) of the Nigeria Data Protection Rules, 2019, the interpretation of any fundamental right provided therein would only be for the purpose of expanding and not restricting same, it is irrelevant that the scope of privacy of citizens as used in section 37 of CFRN, 1999 remains undefined. Such a scope will undoubtedly include the privacy

[14] *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v. NIMC* (2021) LPELR-55623(CA) (pp. 25- 27 paras. E)

and protection of the personal data of citizens as rightly held by the Court of Appeal.

The consequence or significance of the dictum above *inter alia* is that the right to privacy guaranteed in section 37 of CFRN, extends to anything that is private and personal, including personal communication and personal data. In the context of artificial intelligence, this provision is crucial. Artificial Intelligence technologies often involve the collection and processing of vast amounts of personal data, which can erode individuals' right to privacy. The provision reemphasized in the case above, guarantees that citizens' personal data is protected, and any attempts to infringe on this right will be interpreted in favor of the individual. This is particularly important in Nigeria, where Artificial Intelligence technologies are increasingly being used in various sectors, including finance, healthcare, and education. The Court by the above authority explicitly expanded the interpretation of section 37 of the Constitution to include privacy of data even though, the Constitution itself and the Nigerian Data Protection Regulation were clear about the extent to which the right to privacy may be applied. This signifies the classification of data privacy rights as fundamental human rights, capable of being enforced under the Fundamental Rights Enforcement Procedure rules, 2009, and the Constitution.

By interpreting the right to privacy as provided by section 37 of the Constitution to include the right to data protection, the Appellate Court strengthened the capacity to enforce these rights even in the realm of Artificial Intelligence where Artificial Intelligence technologies are deployed for surveillance and data profiling. Thus, the question of whether data privacy and data protection is envisaged by the Constitution is effectively put to rest, positively contributing to the Nigerian jurisprudence in that respect.

3.2 Julius v FRN[15]

In the suit, the Appellant challenged the Federal High Court's judgment, delivered by Hon. Justice A. A. Okeke on January 24, 2020, which convicted and sentenced the appellant under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The Appellant faced a seven-count charge, including computer-related forgery, fraud, cyberstalking, cybersquatting, and racism/xenophobia, to which the Appellant pleaded 'not guilty'. At trial, the respondent presented one witness, while the appellant testified in his defense, along with a second witness. After closing arguments, the trial court convicted the appellant on counts 1-6, but acquitted him on count 7. Dissatisfied with the judgment, the appellant appealed to the Court of Appeal.

In the final analysis, the Court of Appeal found the accused guilty as charged in count 3 for disseminating an unverified information in his Nasarawa Mirror Facebook Platform with the intent that the unsuspecting public would believe and act on same as if it was authentic or genuine. He was not found guilty as charged in the rest of counts 1, 2, 4, 5, 6 and 7. The sentence and conviction of the appellant by the learned trial Judge on counts 1, 2, 4, 5 and 6 respectively were quashed. Appellant's conviction on count 3 was affirmed and he was sentenced to a term of 3 years imprisonment or an option of N7, 000,000.00 fine, thereby varying the 5-year jail term with no option of fine handed down the appellant by the learned trial Judge. In reaching its final decision, the Court of Appeal considered various legal issues, pertinent to this discourse of which are summarized as follows:

a. Objectives of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015
b. Criminalization of formulation of unauthentic data in any computer or network with the intention that such unauthentic data be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.
c. Electronic misrepresentation of facts with intent to defraud.

a. Objectives of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015
On the objectives of the Cybercrimes Act, the Court of Appeal held thus:[16]
It will thus be worth the while to first of all look at the objectives of the Cybercrimes Act

[15](2021) LPELR-54201(CA)
[16] *Julius v FRN* (n 15)

supra, before deciding whether the appellant was rightly or wrongly convicted under the said Act. In order to achieve this, I shall have recourse to the provisions of Section 1 thereof which deals with the objectives of the Act and same is hereby reproduced: 1. (1) The objectives of this Act are to - (a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; (b) ensure the protection of critical national information infrastructure; and (c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

From the holding of the Appellate Court, it is clear that the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, is a comprehensive legislation aimed at preventing and punishing cybercrimes in Nigeria. With the rapid growth of Artificial Intelligence, this Act has significant implications for human rights in terms of the right to privacy and data protection given the concentration of Artificial Intelligence systems on electronic and computer networks and the necessity for an enlarged cybersecurity framework in the face of Artificial Intelligence.

b. Criminalization of formulation of unauthentic data in any computer or network with the intention that such unauthentic data be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.
The Court in the case under review held as follows on the formulation of unauthentic data in a computer or network for the purpose of deceit:
By the provisions of Section 13 of the Cybercrimes Act supra: 13. A person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in unauthentic data with the intention that such unauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than N7,000,000.00 or both. It is pertinent to point out that, access under the foregoing Section 13 of the Cybercrimes Act, supra is not limited to designated computer systems or networks alone. Rather, any person such as the appellant who accesses any computer or "Access Device" such as the appellant's smart phone which was used to input and disseminate or share the vexed information/comment, shall be committing an offence where such information or comment is found to be inauthentic or false.

The above ratio reinforces the questions on liability for false information passed by Artificial Intelligence technologies. Users of Artificial Intelligence technologies such as ChatGPT, Meta AI, *etcetera* can attest that these systems may offer false information or provide erroneous search results to prompts. While the absence of *mens rea* may be argues to exculpate Artificial Intelligence developers, the principle of vicarious liability still applies to make them liable for such dales information disseminated by their Artificial Intelligence systems and programs. Section 13 of the Act as interpreted by the instant case, thus expands the jurisprudence on cybercrime as may be applied to the use of Artificial Intelligence in our polity.

c. Electronic Misrepresentation of Facts with Intent to Defraud
The interpretation of the Court on electronic misrepresentation of facts with intent to defraud may be applied to the interface between artificial intelligence and especially the right to privacy and freedom from misinformation. The Court held in this respect thus:
...Section 14(2) of the Cybercrimes (Prohibition, Prevention etc.) Act, 2015. The Section is reproduced hereunder for ease of reference and it reads: (2) A person who, with intent to defraud, sends electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and is liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than N10,000,000,00 or both. Regarding the essential ingredients required in proving the said count 4, the prosecution has to satisfy

> *the Court that the defendant (appellant): i. with intent to defraud sent by electronic means, message which ii. materially misrepresents any fact or set of facts; iii. that the recipient of such message or any other person relied on it; and iv. as a result of such reliance, the recipient or that other person suffered any damage or loss. All 3 (three) foregoing conditions must be met for the prosecution to make a head way in the count.*

In the context of Artificial Intelligence, this section is essential for safeguarding the right to privacy and freedom from misinformation. Artificial Intelligence algorithms can spread misinformation quickly, and this section as interpreted by the Court in *Julius v FRN*[17]helps hold individuals and organizations accountable for spreading false information.

3.3 Incorporated Trustees of Media Rights Agenda v National Broadcasting Commission[18]

The EndSARS protests in 2020 sparked a significant debate on freedom of expression and press freedom in Nigeria. One of such debates took shape in *Incorporated Trustees of Media Rights Agenda v National Broadcasting Commission*.[19]When television stations reported on the protests, the National Broadcasting Commission (NBC) fined them under the Nigeria Broadcasting Code. However, the Media Rights Agenda challenged this decision in the Federal High Court, arguing that it infringed upon the rights to freedom of expression and the press guaranteed by the Nigerian Constitution and the African Charter on Human and Peoples Rights. The court ultimately ruled in favor of the Media Rights Agenda, declaring that the NBC's imposition of fines without giving the broadcast stations a chance to defend themselves breached the principle of fair hearing and contravened the right to freedom of expression, press, and media. The court also nullified the NBC's authority to impose fines on broadcast stations, emphasizing that regulation must be within the confines of the law. While the Court found the Applicant to have the *locus standi* to bring this suit, the Court went ahead to find that the crux upon which the Applicant based the fundamental rights is predicated on speculation.

The suit is relevant to the discourse on the interaction of Artificial Intelligence with Human Rights to understand how censorship may inhibit the rights to freedom of expression. Unfortunately, the Court did not avail itself the opportunity to consider and fully determine the crux of the Applicant's fundamental rights complaint with respect to the right to freedom of expression and the press by the National Broadcasting Commission fining the stations under the Nigeria Broadcasting Code for airing the protests. In the context of artificial intelligence, there are reports of the use of Artificial Intelligence to remotely inhibit the right to freedom of expression of social media users. The decision herein may be applied as judicial precedent in enforcement of such rights even where the violators are Artificial Intelligence systems or programs.

3.4 The Registered Trustees of the Socio–Economic Rights and Accountability Project (SERAP) v Federal Republic of Nigeria[20]

On June 4, 2021, the Nigerian government announced an indefinite suspension of Twitter, prompting the Socio-Economic Rights and Accountability Project (SERAP) to file a suit at the Community Court of Justice (ECOWAS Court). SERAP challenged the suspension, arguing it infringed upon Nigerian citizens' digital rights, particularly freedom of expression online.

SERAP also sought interim measures to prevent the government from intimidating or harassing citizens using Twitter despite the suspension. The Court ultimately agreed with SERAP, recognizing that denying internet access infringes upon the right to freedom of expression, as guaranteed by the African Charter on Human and People's Rights. The Applicant also filed along with the substantive suit, an application for interim provisional measures seeking to restrain the federal government of Nigeria from intimidating

[17] *Julius v FRN* (n 15)
[18] Unreported Suit No. FHC/IB/CS/101/2020, judgment delivered on 23/06/2021 by J.O. Abdulmalik J at Federal High Court of Nigeria, Ibadan Judicial Division
[19] Ibid
[20] Unreported Suit No. ECW/CCJ/APP/23/21, Ruling delivered on 22/06/2021 by J Gberi–Be Outattara J, Keikura Bangura, Januaria T, Silva Moreira Costa & Mr. Athanase Atannon Community Court of Justice of the Economic Community of West African States(ECOWAS) Abuja

or harassing citizens using the Twitter app in spite of the suspension of its activities in Nigeria.
On the effect of denial of access to Internet on the right to freedom of expression, the Court agreed with the Applicant's Counsel that the cause of action in this matter borders on freedom of expression which is recognized by the African Charter on Human and People's Rights to which the Respondent/Applicant is a party. The Court on this point ruled thus:

> *Access to the internet though not a right, in the strict sense, serves as a platform in which the rights to freedom of expression and freedom to receive information can be exercised, "therefore a denial of access to the internet or to services provided via the internet, as a derivate right, operates as denial of the right to freedom of expression and to receive information.*

This was adequately captured by the Court in its previous decision as follows:

> *Twitter provides a platform for the exercise of the right to freedom of expression and freedom to receive information, which is fundamental human right and any interference with the access, will be viewed as an interference with the right to freedom of expression and information. By extension such interference will amount to a violation of a fundamental human right which falls within the competence of this Court pursuant to Article 9 (4) of the Supplementary Protocol (A/SP.I/ OI /05) amending the Protocol (A/Pl/7/91) relating to the Community Court Of Justice. Evidently, this situates the claim before the Court as one bordering on the Violation of human rights which has occurred in a Member State.*[21]

This decision is a landmark development to the human right jurisprudence in Africa. Most especially the decision of the court recognizing that denial of access to the Internet or to services provided via the internet, as a derivate right, operates as denial of the right to freedom of expression and to receive information.[22] The Courts have gradually begun to appreciate digital rights, even on those enforceable in the realm of social media use, a deviation from times when only traditionally erupting violations may have been considered by our Courts. This is an advantage for the coming times when Artificial intelligence is expected to permeate the digital space, revolutionizing the purport of rights that are enforceable in the Nigerian jurisdiction.

4. Landmark Foreign Decisions on AI Related Human Rights Issues

4.1. Google LLC v Commission Nationale De L'informatique et des Libertés (CNIL)[23]

This suit was heard before the Court of Justice of the European Union (CJEU). The case was heard on the 'right to be forgotten'[24] which is a subsidiary right to the right to data privacy. The right involves the removal of links to web pages from the list of results displayed following a search conducted of the requester's name. It enables any individual to demand that a search engine operator removes certain results linked to his or her name and surname from search results. This removal does not imply the deletion of the information on the initial website. Such a request may only be made by natural persons who are citizens of the European Union and only to remove access to web pages that contain personal information about the requester.

The facts of the case are as follows:
On May 21, 2015, the president of the Commission nationale de l'informatique et des libertés (French Data Protection Authority or CNIL) issued Google a notice directing it to ensure that granted de-referencing requests are carried out on all of Google's domain name extensions worldwide. Google refused to comply with the notice, arguing that the Google Spain decision did not entitle the CNIL to mandate worldwide de-referencing. Google instead confined the scope of de-referencing to domain

[21] S Okedara, O Babalola & I Chukwukelu (Eds), 'Digital Rights in Nigeria: Through the Cases' (2022) <https://digitalrightslawyers.org/wp-content/uploads/2022/09/Digital-Rights-in-Nigera-Through-The-Cases_compressed.pdf> accessed 28/10/2024
[22] Ibid
[23] (2019) EU:C: 2019:772
[24] EU General Data Protection Regulation 2016/679 (GDPR), Art 17

names corresponding to versions of its search engines in EU member states. In response to the concern that internet users could access another version of Google's search engine corresponding to a non-member state to get around de-referencing requests, Google proposed a "geo-blocking" solution that would prohibit an internet user located in a member state from seeing de-referenced web pages regardless of the version of Google they accessed. The CNIL regarded this proposal, which was made after the expiration of the time limit set out in the May 2015 notice, as insufficient and fined Google €100,000 on March 10, 2016. Google sought the annulment of this fine by application to the Council of State.

The European Union advocate general delivered his opinion on January 10, 2019, which argued that while "worldwide de-referencing may seem appealing on the ground that it is radical, clear, simple and effective, it was not apparent from the wording of Directive 95/46 and the Google Spain decision that the "right to be forgotten" required de-referencing on a worldwide scale. On a more practical level, the advocate general suggested worldwide de-referencing could initiate a "race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale, as non-EU countries impacted by worldwide de-referencing could, in response, also implement worldwide de-referencing under their own laws. Furthermore, the advocate general suggested that the objective and practical effect of Directive 95/46 was that de-referencing had to take place on an EU-wide level and that search engine operators had to take all technically feasible steps to ensure effective and complete de-referencing which, in this case, included geo-blocking.

The Court of Justice of the European Union (CJEU or Court) held that the European Union law only requires valid "right to be forgotten" de-referencing requests to be carried out by a search engine operator on search engine versions accessible in European Union member states, as opposed to applying same to all versions of its search engine worldwide.

The ruling which still admits of certain exceptions that restrict requests for de-referencing of individual data where 'public interests' are in issue, has been lauded as a "win" for Google and other interveners, such as Microsoft, who argued against worldwide de-referencing, but is antithetical to privacy rights of individuals. Same has however been excused under the principles of territorial jurisdiction restricting the Court from extending its powers to non-member States. Questions have been raised with respect to balancing the right of a data subject to be forgotten (or data privacy rights) with a third party's right to freedom of information. The CJEU's judgment is likely to have a significant impact not only on the operation of Google's search engine, but on the global digital privacy landscape as a whole.[25]

4.2 State of Vermont v Clearview AI, Inc. Case No. 226-3-20 Cncv[26]

This case is an ongoing case involving the use of facial recognition technology. The State of Vermont sued the defendant, Clearview AI, Inc., alleging that the company's use of that technology constitutes unfair and deceptive acts in commerce in violation of the Vermont Consumer Protection Act. The Plaintiff's claim was that the defendant unlawfully acquires data from consumers and business concerns in Vermont and easily accessible facial recognition would present risks to civil rights, even as they may be inaccurate. The plaintiff alleged that the defendant amassed over three billion photographs from websites around the world and was commercializing same while failing to provide the level of data security proportionate to the sensitivity of data collected.

As if the allegations of data privacy violations were not sufficient, the defendant moved to compel the production of documents from "Vermont law enforcement agencies" and "Vermont agencies." Unfortunately for the defendant, the case is brought in the name of the State of Vermont on behalf of the citizens of the state and not on behalf of state agencies, unlike in cases where the Attorney General is on behalf of a State specifically asserting the interests of various state agencies.[27]

[25] I B Vanderbilt & M Hakimi (Eds), 'Google LLC v. Commission Nationale De L'informatique Et Des Libertés' (CNIL), [2020] (114)(2), *American Journal of International Law*, 261-267.
[26] Ibid
[27] *State v Purdue Pharma*, L.P., No. D-101-CV-2017-02541, 2020 WL 13566522, at *2 (N.M. Dist. July 22, 2020)

The resolution of the issues submitted for determination by the State of Vermont will play a crucial role in the development of the data privacy framework in the face of Artificial Intelligence. This resolution will contribute to the development of a plan of action for regulating the use of Artificial Intelligence in Nigeria with a view to protecting human rights.

5. Evaluation of Judicial Reasoning on AI's Impact on Human Rights

The growing integration of artificial intelligence into various sectors has prompted legal systems to confront complex questions surrounding its implications for fundamental rights. Courts across different jurisdictions have begun to engage with the intersection of Artificial Intelligence technologies and human rights, shaping emerging norms through their interpretations and decisions. This section critically evaluates the judicial reasoning adopted in select cases to assess how courts are responding to the human rights challenges posed by Artificial Intelligence, with a focus on freedom of expression, data privacy, and due process. The analysis highlights both the progress and the limitations in current judicial approaches as they attempt to safeguard rights in an increasingly digital and algorithm-driven society.

5.1 Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC[28]

In *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC*,[29] the *raison d'être* or judicial rationale underpinning the Court of Appeal's judgment lies in the interpretative expansion and constitutional contextualization of the right to privacy under Section 37 of the 1999 Constitution. At the core of the court's reasoning was the recognition that although the Constitution does not explicitly define the term "privacy of citizens," the concept is inherently broad and must evolve in line with contemporary societal realities including the digitalization of identity and personal information management.

The appellate court's affirmation that data protection and informational privacy form part of the general right to privacy, despite the absence of an express textual mention in the Constitution, was an effort in purposively interpreting Constitutional provisions that aim to protect the private sphere of the individual. The court's decision functions as a progressive reaffirmation of data protection as a subset of constitutionally guaranteed privacy rights, capable of enforcement under the Fundamental Rights (Enforcement Procedure) Rules, 2009.

This judicial reasoning contributes significantly to Nigerian data rights jurisprudence by anchoring data privacy within the constitutional framework of fundamental rights; validating the enforceability of such rights even in the absence of express statutory codification; and providing a normative foundation for future legal challenges involving digital identity, surveillance, or data profiling — including those arising from the deployment of artificial intelligence technologies. Thus, the court's rationale reflects both a constitutional safeguarding of individual autonomy in the digital age and a jurisprudential expansion of Nigeria's human rights doctrine to accommodate emergent technologies and data-driven governance.

5.2 Judicial Rationale in Julius v FRN[30]

The judicial rationale sustaining the Court of Appeal's decision in Julius v. FRN rests fundamentally on a purposive interpretation of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, in alignment with the constitutional and legislative objective of safeguarding digital communication channels from manipulation, deception, and harm. The Court's central aim was to uphold the integrity of online spaces and reinforce the deterrence of cyber-enabled offences, especially those involving the dissemination of false, manipulated, or malicious electronic information. The Court acknowledged that Section 1 of the Cybercrimes Act serves as a comprehensive framework not only for criminalizing specified acts within cyberspace but also for protecting public confidence in electronic communications and digital data systems. By affirming the conviction on Count 3, the Court signaled its intent to uphold legislative safeguards against the deliberate spread of unauthentic digital content which could mislead the public or damage reputations conduct which, if left unchecked, would undermine public trust and the sanctity of

[28] *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC* (n 13)
[29] (2021) LPELR- 55623(CA)
[30] *Julius v FRN* (n 15)

online discourse. Moreover, the Court emphasized that Section 13 of the Act, which criminalizes the formulation of unauthentic data intended to be perceived as genuine, applies broadly to all users of electronic platforms including personal devices like smartphones. This interpretation was driven by a policy imperative to establish a technology-neutral standard of liability, ensuring that digital misconduct is punishable regardless of the platform or medium used. This reflects the judiciary's commitment to upholding the rule of law in an evolving digital environment where individuals increasingly rely on online information for civic, political, and economic decisions.

Thus, the raison d'être of the Court's decision can find its basis in the protection of public order, digital trust, and the prevention of misinformation, all while preserving the fundamental rights of the accused by ensuring that each charge is subjected to strict evidentiary scrutiny.

5.3 Judicial Rationale for Court's Decision in Media Rights Agenda v NBC[31]

The judicial rationale behind the Federal High Court's decision in this case lies on the constitutional imperative to uphold freedom of expression and the press, as enshrined in Section 39 of the 1999 Constitution and Article 9 of the African Charter on Human and Peoples' Rights. As seen above, the Court found that the National Broadcasting Commission's unilateral imposition of fines on TV stations for their coverage of the EndSARS protests constituted a violation of the right to fair hearing and exceeded the NBC's statutory powers.

The ruling affirmed that administrative sanctions affecting fundamental rights must comply with due process, and that regulatory overreach cannot substitute for judicial process. While the Court found the Applicant to have *locus standi*, it held that the core human rights claims were speculative, thereby leaving certain substantive issues on press freedom unresolved.

Nonetheless, the decision affirms a crucial precedent - regulatory actions that suppress speech must be legally justified, procedurally fair, and proportionate. This is particularly significant in the context of Artificial Intelligence, where automated censorship or algorithmic moderation by state or private actors can infringe on expressive freedoms. The Court's emphasis on legality and fair hearing provides a basis for extending accountability to AI-driven content regulation, reinforcing the need for transparency and due process in digital governance.

5.4 Judicial Rationale in SERAP v Federal Republic of Nigeria[32]

The ECOWAS Court's decision in this case was founded in the recognition that freedom of expression and access to information, as guaranteed by Article 9 of the African Charter on Human and Peoples' Rights, are central to democratic participation in the digital age. The Court affirmed that while internet access is not itself an independent right, it functions as a derivative enabler for the exercise of fundamental rights such as freedom of expression and the right to receive information. In ruling against Nigeria's indefinite suspension of Twitter, the Court held that blocking access to an online platform constitutes a violation of freedom of expression, particularly where such restriction is not proportionate, legal, or necessary in a democratic society. The Court also granted interim measures to restrain the government from harassing or intimidating citizens for continued use of Twitter, reinforcing the right to access digital platforms free from state coercion.

This case marks a judicial turning point in African human rights jurisprudence, explicitly acknowledging digital rights as enforceable claims. It provides foundational legal grounding for future disputes involving Artificial Intelligence systems that may suppress or filter online expression. As Artificial Intelligence increasingly mediates digital communication, the principles affirmed in this case can be extended to ensure that AI-driven censorship or denial of access is subject to human rights scrutiny and judicial oversight.

[31] *Media Rights Agenda v NBC* (n 18).
[32] *SERAP v Federal Republic of Nigeria* (n 20).

5.5 Judicial Reasoning in Google LLC v CNIL[33]

In Google LLC v. CNIL, the Court of Justice of the European Union (CJEU) considered the scope of the "right to be forgotten" under EU data protection law. The core issue was whether a valid de- referencing request-whereby a search engine removes links associated with a person's name-must apply worldwide or be limited to EU-based search engine domains.

The Court held that EU law (specifically Directive 95/46/EC) does not require search engine operators to implement de-referencing globally. Instead, such requests must be effectively implemented within the EU, using measures such as geo-blocking to prevent access by users in EU member states, regardless of the domain used. The Court emphasized that enforcing global de- referencing would disproportionately interfere with freedom of expression and access to information in jurisdictions not party to the EU legal framework.

The CJEU's ruling upheld the principles of territorial jurisdiction, striking a balance between data privacy rights and the right to information. While seen as a victory for Google and other digital platforms concerned about extraterritorial regulation, the decision also reveals a jurisdictional tension in the enforcement of digital rights, particularly when data circulates across borders.

The case highlights the growing legal challenge of determining the geographic reach of data protection and privacy enforcement, especially as Artificial Intelligence systems aggregate, process, and generate personal data across jurisdictions. The Court's reasoning lays a foundation for reconciling AI-driven data practices with the territorial limits of privacy regulation, particularly as AI amplifies the risks of personal data circulation and profiling at scale.

5.6 Judicial Reasoning in State of Vermont v Clearview AI, Inc[34]

This case is ongoing. It underscores the urgent regulatory gaps in the governance of AI-powered surveillance technologies, particularly regarding data acquisition, biometric privacy, and commercial exploitation of sensitive personal data. The outcome is expected to shape U.S. and possibly transnational standards on the responsible use of FRT by AI companies. For jurisdictions like Nigeria, which are in the process of developing AI regulatory frameworks, the case presents a cautionary precedent on the need to legally delimit AI's intrusion into individual rights, especially with respect to consent, proportionality, and data minimization principles in digital identity systems and law enforcement applications.

6. Conclusion

It is pertinent to observe that given that Artificial Intelligence is a global phenomenon, its regulation requires international cooperation as well as National legislative effort for the formulation of indigenous policies which take the peculiarity of each jurisdiction into consideration. Divergent regulatory approaches and standards across countries can lead to conflicts and inconsistencies, hindering effective governance, further emphasizing the need for international cooperation for effective Artificial Intelligence governance. The regulation of Artificial Intelligence, technology, and human rights is a complex but essential endeavor, simplified only by existing international human rights principles and treaties. Legal and institutional frameworks exist which must evolve to address the ethical and human rights challenges posed by Artificial Intelligence, while developing effective measures by which human rights can amply benefit from emerging technologies including artificial intelligence. International cooperation, adaptive regulatory approaches, and robust enforcement mechanisms are key to ensuring that Artificial Intelligence technologies are developed and deployed in ways that respect and promote human rights.

There is presently a rectifiable insufficiency of laws and regulations that are existing and adaptable to reflect an understanding of the progressive nature of Artificial Intelligence, thus providing an ongoing challenge for the legislature, Courts and civil societies in Nigeria and the wider world. This insufficiency

[33] *Google LLC v CNIL* (23)
[34] *Vermont v Clearview AI, Inc* (n 26)

reflects on the sparse or non-existent body of judicial authorities on the subject matter in Nigeria. As Artificial Intelligence continues to permeate various aspects of life, a balanced and proactive regulatory framework will be crucial in safeguarding individual freedoms and fostering a just and equitable society.

7. Recommendations

In light of the above, the following recommendations are proffered:

i. There is an urgent need for jurisdictions to enact comprehensive legislation that explicitly governs the deployment of Artificial Intelligence technologies in ways that align with human rights standards, defining permissible uses of Artificial Intelligence, imposing obligations on developers and deployers, and providing remedies for rights violations.

ii. Regulatory authorities should support the establishment of independent oversight bodies empowered to monitor Artificial Intelligence systems for human rights compliance. These bodies should have the authority to conduct audits, enforce compliance, and impose sanctions such as exemplified in Incorporated Trustees of Media Rights Agenda v. NBC.[31]

iii. To ensure robust and informed adjudication, judges and legal practitioners should receive continuous training on the technical, ethical, and societal implications of Artificial Intelligence.

iv. Given the opaque and automated nature of many Artificial Intelligence systems, individuals whose rights have been affected must be guaranteed access to justice, including the right to be heard, to access relevant information, and to challenge automated decisions. Courts should emphasize these safeguards in line with rulings like in the Media Rights Agenda case, [32] where lack of fair hearing was central to the decision.

National courts and jurisdictions should engage in transnational judicial dialogue and draw from regional jurisprudence to interpret and enforce human rights norms, since Artificial Intelligence systems often operate across borders. This will foster a consistent standard of protection against AI-related rights infringements.