African Journal of Legal Research [AJLR] (2025) Vol. 3, No. 2
https://africanjournaloflegalresearch.com [ISSN: 1595 – 5966]

REGULATING DIGITAL CRIME: THE IMPACT OF SOCIAL MEDIA ON CRIMINAL BEHAVIOUR, LAW ENFORCEMENT, AND LEGAL ACCOUNTABILITY IN NIGERIA

Bilikis Ayinla- Ahmad*

Abstract

With the rapid growth of digital platforms, crimes such as cyberbullying, internet fraud, incitement to violence, and digital blackmail have increased, posing new challenges for law enforcement and legal institutions. This paper explores the complex relationship between social media, criminal behaviour, and public law in Nigeria. The study aims to examine how social media facilitates criminal conduct, the legal and procedural hurdles in investigating such offences, and the extent to which Nigeria's current legal framework particularly the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 addresses these realities. Drawing on doctrinal legal analysis and criminological theory, the article assesses the effectiveness of existing laws in balancing law enforcement objectives with constitutional protections such as privacy and free expression. It also investigates the role of social media in shaping public perception and in the rise of digital vigilantism. The findings reveal significant enforcement gaps, jurisdictional issues, and limited investigative capacity within law enforcement. The article concludes by recommending legal reforms, digital literacy initiatives, and the establishment of clearer investigative and evidentiary protocols to ensure a more responsive,

* PhD, Dept of Jurisprudence and Public Law, Kwara State University, Malete.
Email: bilikis.ahmad@kwasu.edu.ng ORCID 0009-0008-0908-6388

rights respecting legal approach to digital era crimes in Nigeria.

Keywords: Legal Accountability, Digital Crime, Social Media, Criminal Behaviour, Law Enforcement

1.0 Introduction

The advent of social media has changed how individuals interact, access information and express themselves. According to Bill Gate "The internet is becoming the town square for the global village of tomorrow."[1] The rapid integration of social media into daily life has fundamentally changed the concept of crime, influencing both the commission of crime and subsequently its investigation by law enforcement. Though these podiums were designed for social interface and connection, they have however become an ironic sword, creating new paths for criminal behavior while concurrently providing law enforcement with unprecedented resources. However, it has also created new avenues for criminal behaviour and has complicated traditional methods of criminal investigation. In Nigeria, the rise in cases of cyberbullying, internet fraud, hate speech, and online harassment reflects a growing trend where criminal activity is increasingly mediated through digital platforms.[2] Social media platforms such as Facebook, Twitter (now X), Instagram, and TikTok are often exploited to commit offences ranging from identity theft and romance scams to incitement and defamation.[3]

---

[1] Bill Gates, Business @ the Speed of Thought: Using a Digital Nervous System (Warner Books 1999) 73

[2]. MO Adebayo, 'Cybercrime and Law Enforcement in Nigeria' (2020) 6(1) Journal of Digital Law and Policy 45.

[3] B Okon, 'The Use and Misuse of Social Media in Nigeria' (2021) African Journal of Criminology 9(2) 87

Social media has progressed briskly from humble online communication kits into intricate podiums that shape general speech, influence political movements, and impact legal systems. Initially, emerging in the early 2000s with sites like Friendster and MySpace, the landscape quickly transformed with the rise of Facebook (2004), Twitter (2006), Instagram (2010), and later TikTok (2016), each offering unique forms of user interaction and content sharing.[4] This evolution has not only enhanced global connectivity but also introduced challenges such as cybercrime, digital misinformation, and privacy breaches.

In Nigeria, the deployment of social media in the perpetuation of criminal activities has become preponderant, especially among young people. This is because social media has emerged as a powerful force in shaping the behaviours and attitudes of youths in Nigeria.[5] Technological advancements, increased smartphone penetration, and affordable internet access have further driven the widespread adoption of these platforms in Nigeria and other developing nations.[6] As social media platforms grew, they became essential tools for civic engagement, activism, business, and even criminal activity, thus attracting legal and academic scrutiny.

[4] Andreas M Kaplan and Michael Haenlein, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' (2010) 53(1) *Business Horizons 59.

[5] Edafe Ulo and Collins Emudiaga Akpumuvie, 'Social Media and Criminality: A Focus on Anonymity and Validity Among Youths in Delta State, Nigeria' (2023) *Sapientia Global Journal of Arts, Humanities and Development Studies (SGOJAHDS). <https://www.academia.edu/108490359/Social_Media_And_Criminality_A_Focus_On_Anonymity_And_Validity_Among_Youths_In_Delta_State_Nigeria> accessed 14 November 2025.

[6]Boma Ndinojuo, 'The Evolution and Impact of Social Media in Nigeria' (2021) 13(2) *Journal of Media and Communication Studies 25.

From a criminological and legal perspective, social media now serves as both a site and a tool for criminal behavior, necessitating new regulatory frameworks and enforcement strategies.[7] This evolution reflects the dual-edged nature of technological advancement enabling positive connectivity while posing governance and legal dilemmas.

From a legal standpoint, Nigeria has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 to address crimes committed through electronic means. Nevertheless, challenges persist in areas such as enforcement, jurisdiction, digital evidence handling, and balancing constitutional rights such as freedom of expression and privacy.[8] Criminologically, the accessibility and anonymity provided by social media often embolden offenders, reduce inhibitions, and facilitate the spread of deviant behaviours, especially among youths.[9]

This article critically examines the intersection of social media, criminal behaviour, and investigation through both legal and criminological lenses. It seeks to evaluate the adequacy of Nigeria's legal framework, the challenges faced by law enforcement, and the broader implications for public safety, legal reform, and digital rights in Nigeria.

2.0 LEGAL FRAMEWORK

The legal framework guiding the connection of social media, criminal behaviour, and investigation in Nigeria is multi-layered. At the core is the

[7]Emmanuel Okon, 'Social Media and Cybercrime in Nigeria: Legal and Regulatory Challenges' (2020) 5(1) *Nigerian Journal of Internet Law* 18.
[8] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 1–8.
[9] AI Ajayi, 'Social Media and Youth Criminal Behaviour in Urban Nigeria' (2019) 12(1) *Nigerian Journal of Criminology* 33

2.1 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, which criminalises offences such as cyberstalking, cyberbullying, identity theft, and the unlawful use of social media for criminal purposes.[10] Section 24 of the Act particularly addresses offensive or harmful communications on social media, while section 27 empowers law enforcement agencies to arrest and prosecute offenders.[11] While the 2015 Act was a monumental step, the ever-evolving nature of cybercrime necessitated continuous review. Recent amendments, such as those introduced in the Cybercrimes (Amendment) Act 2024, aim to strengthen the legal framework further. Key changes include heavier penalties for cybercrimes like hacking and online fraud, stricter punishments for unauthorized cryptocurrency transactions, and increased liability for social media platforms failing to remove "offensive" content promptly.[12]

2.2 The Nigeria Data Protection Act

Beyond prosecuting cybercrime, a critical aspect of digital law involves safeguarding personal data. Nigeria's journey in data protection gained significant momentum with the issuance of the Nigeria Data Protection Regulation (NDPR) 2019 by the National Information Technology Development Agency (NITDA). The NDPR was pioneering in its aim to protect the rights of persons to privacy, foster safe conduct for data transactions, and prevent personal data manipulation.[13] It introduced a compliance model involving Data Protection Compliance Organizations (DPCOs) and mandated data audit reports from data controllers and

[10] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss. 1–44 (n. 8)
[11] Ibid, s. 24; s. 27.
[12]NALTF, 'Nigeria's Cybercrime Reform' (22 May 2025) <https://naltf.gov.ng/nigerias-cybercrime-reform/> accessed 11 December 2025.
[13]National Information Technology Development Agency (NITDA), 'Nigeria Data Protection Regulation (NDPR) 2019' <https://nitda.gov.ng> accessed 11 December 2025

processors.[14] Building on the NDPR's foundation, the Nigeria Data Protection Act (NDPA) 2023 was enacted, elevating data protection to a statutory level and establishing the Nigeria Data Protection Commission (NDPC) as an independent supervisory authority.[15] The NDPA retains many principles of the NDPR, including lawful bases for processing personal data, and introduces enhanced safeguards for children's data.[16] The Act empowers the NDPC to issue guidelines, investigate breaches, and impose penalties for violations, with significant fines stipulated for non-compliance.[17]

2.3 Evidence Act 2011, which recognises electronically generated evidence, including social media content, as admissible in court, provided certain authentication conditions are met.[18] This is crucial for enabling investigators to rely on digital footprints during prosecution.

2.4 Nigerian Constitution, which guarantees fundamental rights such as privacy[19] and freedom of expression.[20] These rights, however, must be balanced with national security interests and public order when social

[14]National Information Technology Development Agency (NITDA), 'Nigeria Data Protection Regulation 2019: Implementation Framework' (January 2021) <https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf> accessed 11 December 2025.
[15]. Nigeria Data Protection Act 2023.
[16] O Adedunmade, 'The Evolving Landscape of Digital Law and Cybercrime in Nigeria' AOC (2025) <https://aocsolicitors.com.ng/the-evolving-landscape-of-digital-law-and-cybercrime-in-nigeria/> accessed 7 November 2025.
[17]Ibid.
[18] Evidence Act 2011, ss 84–93.
[19]Constitution of the Federal Republic of Nigeria 1999, s 37.
[20] ibid, s 39.

media is used to incite violence or spread misinformation.[21] The Supreme Court of Nigeria has stated on many occasions that the right to freedom of expression is not absolute.[22] While section 39(1) of the Nigerian Constitution guarantees the right to freedom of expression, it also recognizes that there may be circumstances where this right needs to be restricted. Section 39(3)(a) provides for such restrictions in cases where the disclosure of information received in confidence or the maintenance of the authority and independence of the courts necessitates it.[23]

The restriction of the right to freedom of expression under the Constitution can be either a general or a specific limitation.[24] A specific limitation is sometimes contained in the section or a subsection that provides for the protection of the free expression right.[25] In Nigeria, Section 45 of the Nigerian Constitution allows for the general limitation of certain fundamental rights outlined in Chapter IV of the Constitution. Section 45 provides:

Nothing in sections 37, 38, 39, 40, 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society:

(a) in the interest of defence, public safety, public order, public morality, or public health; or

[21] Ginikachi Goodness Okewulonu, The Regulation of Social Media in Nigeria and its Effect on Free Speech: Perspectives from Constitutional Law and International Norms (Master's thesis, University of Saskatchewan 2023) <file:///C:/Users/HP/Desktop/OKEWULONU-THESIS-2024%20SOCIA%20MEDIA%205.pdf> accessed 14 November 2025.

[22] Aviomoh v Commissioner of Police & Anor (2021) LPELR-55203 (SC).

[23] The Nigerian Constitution (n 19)

[24] Stephen Gardbaum, 'The Structure of a Free Speech Right' in Adrienne Stone and Frederick Schauer (eds), The Oxford Handbook of Freedom of Speech (Oxford University Press 2021) 213, 221.

[25] Ibid.

(b) for the purpose of protecting the rights and freedom of other persons.[26]

2.5 The Nigerian Communications Act 2003, also plays a role by regulating telecommunications providers and setting standards for data management, which indirectly affects how digital investigations are conducted.[27]

Together, these legal instruments provide a framework for addressing and investigating criminal activity on social media, though enforcement challenges and concerns over human rights abuses persist.[28]

2.6 Criminal Code Act (Southern Nigeria) and Penal Code (Northern Nigeria)

Provide for traditional criminal offences that may now be committed via social media (e.g., defamation, incitement, conspiracy).

2.7 Nigeria Police Act 2020, Guides modern policing techniques, including digital investigation and respect for human rights.

2.8 Regional Frameworks, African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) Encourages member states to regulate digital crimes and protect data.

2.9 International Frameworks, Budapest Convention on Cybercrime (2001) First international treaty seeking to address internet and computer

[26]The Nigerian Constitution, s 45 (n 19)
[27] Nigerian Communications Act 2003, ss. 1–3.
[28] AE Okoro, 'Regulating Social Media: Challenges of the Nigerian Legal System' (2021) 4(2) African Journal of Law and Society 58.

crime by harmonising national laws and improving investigative techniques.

2.10 Universal Declaration of Human Rights (1948) Articles 12 and 19 uphold the rights to privacy and freedom of expression. The Universal Declaration of Human Rights (UDHR) is a significant declaration in the history of protecting fundamental human rights.[29] The UDHR was for the protection of human rights in response to the "barbarous acts which…outraged the conscience of mankind", especially after World War I and II, which ended in 1918 and 1945.[30] Thereafter, the United Nations General Assembly adopted the Universal Declaration of Human Rights by an overwhelming vote in 1948.[31] It was the first time that different countries in the world came together to agree on the protection of fundamental human rights.

The UN General Assembly described the UDHR as "a common standard of achievement for all peoples and all nations" that contains fundamental rights that are universally protected.[32] The UDHR has served directly and indirectly as a model for many international conventions and treaties, as well as many regional conventions and domestic laws.[33]

[29]Universal Declaration of Human Rights (UDHR); International Covenant on Economic, Social and Cultural Rights (ICESCR); and International Covenant on Civil and Political Rights (ICCPR), collectively referred to as the International Bill of Human Rights

[30] Tarlach McGonagle, 'The United Nations and Freedom of Expression and Information' in Tarlach McGonagle and Yvonne Donders (eds), The United Nations and Freedom of Expression and Information: Critical Perspectives (Cambridge University Press 2015).

[31] Universal Declaration of Human Rights, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71

[32] Ibid.

[33]Hurst Hannum, 'The Status of the Universal Declaration of Human Rights in National and International Law' (1996) 25(1) Georgia Journal of International and Comparative Law 287, 289.

The UDHR, among other things, guarantees the right to freedom of expression. Article 19 of the UDHR provides that:

Everyone has the right to freedom of opinion and expression: this right includes freedom to hold opinions without interference and to see, receive and impart information through any media and regardless of the frontiers.

This article provides for the universal protection of the right to freedom of speech, irrespective of race or location.[34] The UDHR has a non-binding force on states and, therefore, cannot be legally enforceable against member states. However, it is still regarded as a declaration with great 'ethical force.'[35] Though Article 19 of the UDHR protects the right to freedom of expression, Articles 29 and 30 of the Declaration provide a general limitation on the provision of the rights protected under the UDHR. Articles 29 and 30 state as follows:

Article 29

(1) Everyone has duties to the community in which alone the free and full development of his personality is possible.

(2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order, and the general welfare in a democratic society.

(3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

and Article 30

[34] Ibid.
[35] Ibid.

Nothing in this Declaration may be interpreted as implying for any State, group, or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.[36]

3.0 The impact of social media

Social media has transformed how people connect and contact information, significantly impacting society. It aids instant distribution of news and opinions, forms public awareness, and effects social and political movements. However, it also permits the fast spread of fabrication, cyberbullying, and digital crimes. In criminal behavior and investigation, social media can both relief law enforcement by providing evidence and intelligence, and confuse matters by nurturing digital vigilantism and privacy concerns. Overall, its impact is insightful, creating new opportunities and challenges for justice systems.

3.1 The role of social media in shaping public perception in the rise of digital vigilantism.

Social media is defined as a "forms of electronic communication (such as websites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)"[37]

Social media plays a major part in determining public awareness by swiftly publicizing material, often by-passing traditional media filters. It provides a platform for factual time sharing of actions, ideas, and rejoinders, which can impact how individuals and communities view criminal incidents and

[36] UDHR (n. 31.)
[37] Merriam-Webster, *Merriam-Webster Dictionary (11th edn, Massachusetts, 2019)

justice processes.[38] However, this proximity sometimes leads to the spread of propaganda or unfair narratives that may tilt public understanding. The rise in the use of social media now have caused more harm than good, making it possible for criminal activities to thrive more via the virtual environment than it does in the physical community. One of the most powerful and successful tools, social media, has suddenly become a haven for criminals. In the last decade, as the number of internet users has grown, so has the number of cybercrimes.[39]

3.2 Types of Digital crimes

3.2.1 Cyber Fraud - This includes phishing, identity theft, and financial scams conducted through emails, fake websites, or social media. It targets individuals and institutions to gain unauthorized financial benefits.[40] The following cases would provide further authority for this menace: FRN v. Emmanuel Nwude & Ors.[41] Also in FRN v. Wilfred Fajemisin (unreported)[42]

3.2.2 Hacking and Unauthorized Access - Illegally accessing computer systems, servers, or databases to steal, alter, or destroy information. This

[38] T Jonathan-Zamir and D Weisburd, 'The Effects of Security Threats on Community Attitudes toward Crime and Policing: The Israeli Case' (2013) 51(4) *Criminology 743–776

[39] T R Sumro and M Hussain, 'Social Media Related Cybercrimes and Techniques for their Prevention' ResearchGate (May 2019) <https://www.researchgate.net/publication/333944511_Social_Media-Related-Cybercrimes-and-Techniques-for-Their-Prevention> accessed 22 September 2025.

[40] M O Adebayo, 'Cybercrime and Legal Response in Nigeria' (2020g) 10(2) Journal of Social and Policy Studies 45 available at https://portal.corruptioncases.ng/judge-cases/339 accessed 14th November, 2025.

[41] unreported case Federal High Court, Lagos 2005

[42] Ibid.

can threaten national security or business operations.[43] See Okedara v. Attorney-General (Lagos) – suit challenging computer-system offence, Federal High Court Lagos (unreported).[44]

3.2.3 Cyberstalking and Online Harassment - Use of digital platforms to stalk, threaten, or harass individuals, often involving repeated unwanted communication or surveillance.[45] It refers to the repeated use of electronic communication (emails, social media, texts, etc.) to stalk or harass an individual, often including threats, false accusations, or monitoring.[46]
Online Harassment includes broader behaviors such as sending offensive messages, publishing defamatory content, impersonation, or spreading harmful rumors online.[47]

3.2.4 Child Pornography and Exploitation, Using the internet to distribute or access materials that sexually exploit children, a serious offense under Nigerian and international law.[48]

3.2.5 Cyberterrorism, The use of digital means to cause large scale disruption, fear, or violence, often targeting infrastructure or spreading

[43] I C Chukwuma, 'Hacking and Digital Intrusions in Nigeria: A Legal Review' (2017) 11(1) African Journal of Criminology 66.
[44] Okedara v Attorney General, Global Freedom of Expression (columbia.edu) <https://globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general> accessed 11 December 2025.
[45] MC Ogwezzy, 'Cyberstalking: A Threat to Personal Liberty in Nigeria' (2019) 6(1) Nigerian Journal of Cyber Law 22..
[46] Section 24(1) Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (n. 8)
[47] IA Aduba , 'Gender Violence and the Challenges of Traditional Norms in Nigeria' (2011) 5(1) Nigerian Journal of Gender and Law 1.
[48].UNODC, Online Child Exploitation and Protection in Africa, United Nations Office on Drugs and Crime Report (2021)

extremist content.[49] Cyberterrorism refers to the use of digital technologies to carry out terrorist activities or cause disruption, fear, or physical harm to individuals, institutions, or governments. This includes hacking critical infrastructure, spreading extremist content, or coordinating attacks through digital platforms.[50]

3.2.6 Online Defamation, Publishing false or harmful information online that damages someone's reputation. Social media has increased the incidence of this.[51] Online defamation occurs when false statements are published on the internet (e.g., via social media, blogs, or websites) that damage a person's reputation. It includes libel (written defamation) and slander (spoken defamation, possibly via audio/video posts online).[52]See Ejike Mbaka v. Sahara Reporters (Unreported).

3.2.7 Cyberbullying, is the intentional and repeated use of digital technologies such as social media, messaging apps, or email to harass, threaten, embarrass, or target an individual or group, particularly among youths. It includes name-calling, spreading false information, sharing private images, or exclusion from online communities. Social media allows for sustained abuse or blackmail, often crossing into criminal behavior.[53]

[49] EEO Alemika, Terrorism and Digital Platforms: Nigerian Experience, CLEEN Foundation Monograph Series (2015) 12.
[50] Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (n. 8), S. 18, Terrorism (Prevention and Prohibition) Act, 2022, Constitution of the Federal Republic of Nigeria 1999 (as amended), s. 45(1)
[51] TU Okonkwo, 'Digital Defamation and Legal Remedies in Nigeria' (2022) 18(2) Nigerian Law Review 55..
[52] Criminal Code Act (s. 373–375), Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (s. 24), Constitution of the Federal Republic of Nigeria 1999 (as amended), s. 39.
[53] Aduba, n 48, p. 1.

In Nigeria, while there is no single comprehensive cyberbullying law, such acts may be prosecuted under sections of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, especially where threats, harassment, or harmful communications are involved.[54] See Attorney-General of the Federation v Ayan Olubunmi[55] see also Ejike v Obi.[56]

3.2.8 Incitement to Violence, refers to speech, writing, or behavior that encourages others to commit acts of violence or unlawful force. It is criminalized because it poses a serious threat to public order, peace, and safety. In the digital age, incitement can occur through social media, blogs, or messaging platforms, often going viral and sparking real-world consequences. In Nigeria, incitement is punishable under both general criminal law and specific legislation such as: Criminal Code Act (Sections 88–90), Penal Code (applicable in Northern Nigeria), Cybercrimes (Prohibition, Prevention, etc.) Act 2015, especially where messages are disseminated online.[57] See FRN v Omoyele Sowore & Another[58], Commissioner of Police v Dikko[59], also FRN v Nnamdi Kanu [60]

3.2.9 Digital Blackmail involves the use of threats via digital platforms such as emails, messaging apps, or social media to extort money, favors, or silence from victims, often by threatening to release sensitive or

[54] AA Adebayo, 'Cyberbullying and Online Safety: A Legal Perspective in Nigeria' (2021) 4(1) Nigerian Journal of Internet Law 34.
[55] (Federal High Ct, Ado-Ekiti, 2017)
[56] (2022) 4 NWLR (Pt 1855) 120.
[57] CU Okonkwo, 'Regulating Online Incitement in Nigeria: Legal and Policy Challenges' (2020) 2(1) Nigerian Journal of Cyber and Criminal Law 55.
[58] (Unreported, Federal High Court, Abuja, 2019)
[59] (2018) 12 NWLR (Pt 1633) 432
[60] Kanu v Federal Republic of Nigeria (2023) LPELR-60587(SC).

compromising information. Digital blackmail is increasingly linked to sextortion, corporate data breaches, and political manipulation.[61] EFCC v Oyekanmi Rasaq.[62] Rasaq was arrested by the Economic and Financial Crimes Commission (EFCC) for threatening to release compromising photos of a woman online unless she paid a sum of money.[63]

3.3 Social media facilitates criminal conduct in several ways:

Social media facilitates criminal conduct in several ways, serving not only as a platform for communication but also as a tool for planning, executing, and concealing unlawful acts. Its real-time nature, wide reach, and perceived anonymity enable activities such as cyberstalking, fraud, blackmail, incitement to violence, and recruitment for criminal enterprises. Criminals exploit loopholes in content moderation and jurisdictional enforcement, making it difficult for law enforcement to trace and prosecute offenders promptly. As digital platforms evolve, so too do the tactics of those who misuse them for criminal gain like:

i. Anonymity and Pseudonymity - Users can hide their real identities, making it easier to commit crimes like fraud, harassment, or threats without immediate detection.[64] Cyberbullying and Harassment, Radicalisation and Incitement and Blackmail and Sextortion.[65]

ii. Wide Reach and Speed, Criminals can quickly spread illegal content, such as hate speech, incitement to violence, or

[61] YO Adebayo, 'Cyber Blackmail and Nigerian Cybersecurity Law: A Critical Appraisal' (2019) 4(2) Journal of Law and Digital Security 72.
[62] (2020) (Unreported)
[63] Cybercrimes Act 2015, s.24(2) (n. 8)
[64] J Smith, 'Anonymity and Crime on Social Media' (2019) 2(3) Cybersecurity Journal 15..
[65] MO Adebayo, (n. 2) 4

misinformation, to large audiences.[66] The internet and social media allow content whether lawful or criminal to be disseminated instantly to millions.[67]

iii. Coordination and Recruitment - Platforms are used to organize illegal activities, recruit members for gangs or terrorist groups, and coordinate crimes.[68]

iv. Fraud and Scams - Criminals use social media for phishing, identity theft, and financial scams by exploiting trust and social connections.[69]

3.4 Legal and Procedural Hurdles in Investigating Digital Crimes

There are several challenging circumstances in investigating criminal crime ranging from Jurisdictional Issues,[70] Lack of Specialized Training,[71] Evidentiary Challenges,[72]Limited Technological Infrastructure, [73] Weak Legal Frameworks or Enforcement Gaps and Victim Reluctance.[74]

[66] I Johnson , 'Social Media and the Spread of Illegal Content' (2020) 5(1) Journal of Digital Crime 9.
[67] B Okon, (n. 3) 87
[68] O A Ogunleye, 'The Role of Social Media in Crime Facilitation in Nigeria' (2018) 4(2) Nigerian Journal of Criminology 33.
[69] A E Adebayo, 'Financial Scams on Social Media Platforms' (2016) 8(1) African Journal of Law 42.
[70]T Akinola, 'Cross-border Cybercrime Investigation Challenges' (2018) 3(1) Nigerian Journal of Cyber Law 45...
[71] J Okeke, 'Training Gaps in Cyber Forensics' (2017) 5(4) Law Enforcement Review 22..
[72] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s. 30 (n. 8)
[73]CLEEN Foundation, Cybersecurity Infrastructure in Nigeria: An Assessment (2019).
[74]NOIPolls, Public Perception of Cybercrime Reporting in Nigeria (2021)..

3.5 Criminological Analysis

The rise of social media has reshaped not only social interaction but also the nature and visibility of criminal behaviour. From a criminological perspective, several theories help explain the link between social media and crime.

Firstly, Social Learning Theory posits that individuals can learn deviant behaviour through observation and imitation, especially when such behaviour is rewarded or normalised online.[75] Social media platforms amplify this by providing constant exposure to criminal acts, cyberbullying, internet fraud, and glorification of violence.

Secondly, the Routine Activity Theory explains how crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian.[76] Social media creates the perfect conditions offenders can easily identify vulnerable users (targets) and exploit the lack of real-time monitoring (guardianship) to commit cybercrimes such as sextortion, scams, and threats. [77]

Thirdly, Anonymity and disinhibition facilitated by social media platforms contribute to deviant behaviour. Users may feel detached from the consequences of their actions, leading to more aggressive or illegal conduct, such as online harassment and hate speech.[78]

[75]Bandura Albert, Social Learning Theory (Prentice Hall 1977) 22..
[76]L E Cohen and M Felson, 'Social Change and Crime Rate Trends: A Routine Activity Approach' (1979) 44(4) American Sociological Review 588.
[77]E Akpan, 'Social Media, Violence and Youth Criminality in Nigeria: A Criminological Review' (2020) 8(1) Nigerian Journal of Criminology 45.
[78]J Suler, 'The Online Disinhibition Effect' (2004) 7(3) CyberPsychology & Behavior 321.

Overall, criminological theories provide essential insight into the psychological and social dynamics of how and why individuals engage in criminal acts via social media. Understanding these patterns is key to developing effective preventive and investigative strategies.

4.00 Law Enforcement and Investigation

The proliferation of social media has significantly transformed the landscape of criminal investigations and law enforcement operations. Digital platforms now serve as both crime scenes and tools for detection, presenting unique challenges and opportunities. [79]

Social media has become a rich source of intelligence gathering. Law enforcement agencies often monitor platforms for real-time information, suspect identification, and evidence collection.[80] Posts, images, location data, and even live videos can offer critical leads in ongoing investigations. However, this digital shift also raises legal and ethical concerns. One major issue is the admissibility of social media evidence in court, which depends on proper authentication and compliance with evidentiary rules.[81] Unlawfully obtained data, or content gathered without a warrant, may be deemed inadmissible, violating privacy rights under national constitutions and data protection law.[82]

In Nigeria, there is still no comprehensive legislation that clearly regulates digital surveillance by law enforcement. The Cybercrimes (Prohibition,

[79] U Akpojivi, 'Policing and Social Media in Nigeria: Rights, Risks, and Regulation' (2021) 3(1) African Journal of Law and ICT 57.
[80]D Trottier, Social Media as Surveillance: Rethinking Visibility in a Converging World (Ashgate 2012) 118.
[81]S Mason, Electronic Evidence (4th edn, Institute of Advanced Legal Studies 2017) 231.
[82] The Nigerian Constitution, s. 37 (n. 19)

Prevention, etc.) Act 2015 provides some framework, but enforcement is inconsistent and sometimes abused.[83]

4.1 Related Cases on social media and criminalities

In recent years, courts in Nigeria and beyond have increasingly encountered cases where social media platforms play a central role in the commission, facilitation, or investigation of crimes. From cyberbullying and online fraud to incitement and defamation, these cases highlight the growing intersection between digital expression and criminal liability. Judicial decisions now shape how evidence obtained online is admitted, how freedom of speech is balanced with public order, and how law enforcement navigates the legal boundaries of digital surveillance and privacy rights. Examples of related cases are as follows: see Federal Republic of Nigeria v. Sowore et al,[84] Federal Republic of Nigeria v. Scott Iguma, FHC Lagos,[85] State v. Paul Ezeugo & Ors.[86], EFCC v. Emmanuel Nwude & Ors[87] FRN v. Joshua Dariye [88] Kubor v. Dickson [89] State v. Nwabufo & Ezike,[90] Director of Public Prosecutions v Elliot[91] U.S. v. Drew.[92]

4.2 Legal Accountability

Legal accountability in Nigeria refers to the obligation of individuals, institutions, and government agencies to act in accordance with the law and

[83] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss. 38–41.(n.8)
[84] FHC/ABJ/CR/484/2025 (FHC Abuja Oct. 27, 2025)
[85] (July 16–21, 2025) (unreported)
[86] (2017) (Lagos State High Court, Igbosere) (death sentence)
[87] (2005) (Unreported, Federal High Court, Lagos, 2005)
[88] (2018) LPELR-45107(SC)
[89] (2013) 4 NWLR (Pt. 1345) 534
[90] Lagos State High Court (Igbosere) (2017) (unreported)
[91] [2013] EWHC 2186 (UK).
[92] (2009) 259 F.R.D. 449 (C.D. Cal. 2009)

face consequences when they violate legal standards. In the context of digital crime and social media, legal accountability involves ensuring that online offenders are prosecuted under applicable laws such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Criminal Code, and other related statutes

4.3 The effectiveness of existing laws in balancing law enforcement objectives

The Cybercrimes Prohibition, Prevention, etc. Act 2015 provide a framework for prosecuting offenses.[93] However, Nigerian Constitution guarantees the right to privacy and freedom of expression which can conflict with aggressive surveillance or content regulation by authorities.[94]For instance, broad powers granted to law enforcement can lead to unlawful interception of communications or censorship, undermining free speech and privacy protections. [95]

Furthermore, vague legal definitions in cybercrime statutes can result in overreach or misuse against legitimate online expression or dissent, creating a chilling effect.[96]

4.4 Lessons from Other Jurisdictions

Several countries offer instructive models Nigeria can learn from in managing the legal and criminological implications of social media in crime and investigation: For instance

[93] Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. (n. 8)
[94] Constitution of the Federal Republic of Nigeria, 1999 (as amended), ss 37 & 39. (n. 19)
[95] CLEEN Foundation, Legal Awareness and Access to Justice Survey Report (2019)..
[96] O Igbuzor, 'Impunity and the Challenges of Cyber Law Enforcement in Nigeria' (2011) 3(1) Nigerian Journal of Law 45.

4.4.1 United Kingdom: The UK has integrated digital forensic units within its police services, and courts admit social media evidence under strict evidentiary rules. The UK's Criminal Procedure and Investigations Act 1996 requires proper disclosure and preservation of digital evidence, ensuring transparency and admissibility.[97]

4.4.2 United States: U.S. law enforcement regularly monitors open source social media for criminal activity. Courts have developed jurisprudence on digital privacy and admissibility, especially post Carpenter v. United States (2018), which emphasises the need for warrants before accessing location data.[98]

4.4.3 India: The Indian judiciary increasingly relies on social media content in criminal trials. However, concerns about misinformation and mob justice have led to calls for regulatory clarity, particularly under the Information Technology Act 2000. India's approach shows the balance between using social media for justice and regulating misuse.[99]

4.4.4 South Africa: South Africa's cybercrime law (Cybercrimes Act 2020) criminalises false information on social media and enables state agencies to gather digital evidence. Their law provides lessons on proactive legislation addressing online criminal behaviour.[100]

[97] Home Office, Criminal Procedure and Investigations Act 1996 (HMSO 1996)

[98] O S Kerr, 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution' (2004) 102(4) *Michigan Law Review 801 in Supreme Court of the United States, *Carpenter v United States 585 US _ (2018)

[99] Government of India, Information Technology Act 2000 (as amended), 2. S Ghosh, 'Law, Social Media and the Indian Legal System' (2016) 3(2) Indian Journal of Law and Technology 45..

[100] Republic of South Africa, Cybercrimes Act 19 of 2020, J Burchell, 'Cybercrime and the Law in South Africa' (2021) 33(1) South African Journal of Criminal Justice 1

5.0 Summary of Findings

The rapid evolution of digital technologies has overtaken the development of clear legal standards governing their use by both individuals and law enforcement agencies. The effectiveness of the cybercrime Act continues to be debated, with challenges such as weak enforcement, jurisdictional complexities, and limited technical expertise often cited as hindrances to its full impact. difficulty in tracking offenders due to encrypted apps and anonymous platforms.

i. Lack of specialised digital forensic units and child protection officers as well as inconsistent application of the Child Rights Act across all states.
ii. There seems to exist conflict between freedom of expression and protection from harm.
iii. Jurisdictional issues when defamatory content originates from outside Nigeria.
iv. The absence of comprehensive digital evidence laws, the available laws only provide general guidance but lack specificity regarding the collection, preservation, and admissibility of evidence sourced from social media.

It was found that Nigeria lack a regulatory body as oversight for law enforcement surveillance. There are limited mechanisms to ensure accountability for how police or security agencies access and use digital content. Additionally, Nigeria is yet to domesticate global data protection standards such as the General Data Protection Regulation (GDPR), leading to weaker enforcement. Moreover, social media companies themselves operate with limited regulatory oversight, often resisting requests for data or failing to act promptly on content that incites violence or facilitates

criminal behavior.[101] This complicates criminal investigations and hinders efforts to hold platforms accountable for harmful content.

Finally, public trust in the criminal justice system is affected when social media evidence is perceived to be manipulated or selectively used by authorities, especially in high profile cases. Without transparent policies and clear judicial review procedures, the legitimacy of social media use in criminal justice remains contested.[102] These legal vacuum leads to inconsistencies in judicial decisions and undermines defendants' rights to fair trial protections under Constitution.[103]

6.0 Conclusion

The increasing influence of social media on both criminal behaviour and investigative processes presents significant legal and criminological challenges in Nigeria. While platforms such as Facebook, X (formerly Twitter), and Instagram have become tools for facilitating, publicising, or even glamorising criminal conduct, they have also emerged as valuable sources of intelligence and evidence for law enforcement agencies. However, the absence of specific legal frameworks, limited digital forensic capacity, and concerns around privacy and due process hinder effective and lawful use of social media in criminal justice administration.

A balanced approach is therefore required one that respects constitutional rights while enhancing investigative efficiency. Legal reforms, improved

[101] U Akpojivi, 'Policing and Social Media in Nigeria: Rights, Risks, and Regulation' (2021) 3(1) African Journal of Law and ICT 63.
[102] S Adebanjo, 'Social Media Evidence and Criminal Justice in Nigeria: A Case for Reform' (2022) 14(2) Nigerian Law Review 101.
[103] Constitution of Nigeria 1999 s.36. (n. 19)

law enforcement training, robust data protection mechanisms, and greater public awareness are necessary to ensure that the use of social media in the criminal justice system promotes justice rather than undermines it. As Nigeria continues to navigate the digital era, it must build a legal and institutional framework that is responsive to the complexities of cyber enabled crime and the opportunities offered by digital evidence.

7.0 Recommendations

The following recommendations are apposite:

i. There is need to enact clear digital evidence laws to guide admissibility and handling.
ii. There is need to build digital forensic and cybercrime units within police structures.
iii. Training and retraining for judicial officers and Law enforcement agencies on interpreting social media related evidence.
iv. There is need to introduce safeguards to protect digital privacy and avoid abuse.
v. There is a need to fully implement and enforce Nigeria's Data Protection Act 2023.
vi. Independent oversight bodies should be established or reinforced to monitor digital surveillance.
vii. There is need for technological integration in judicial processes and formal partnerships with major social media platforms
viii. Promoting public awareness and digital literacy
ix. Nigeria can learn from other countries models as discussed herein in managing the legal and criminological implications of social media in crime and investigation.