

## DIGITAL FOOTPRINTS AND CRIMINAL LIABILITY: LEGAL AND CRIMINOLOGICAL PERSPECTIVES.

Dr Bilikis Ayinla- Ahmad \* & Olateju Olatunbosun Gideon \*\*

### Abstract

*This paper examines how social media both facilitates criminal behaviour and transforms criminal investigation, with attention to legal and criminological implications for Nigeria and comparative international frameworks. It argues that platforms such as Facebook, Instagram, X, and TikTok create opportunities for offences including fraud, identity theft, cyberstalking, hate speech, grooming, organized-crime coordination, and misinformation by increasing accessibility, anonymity, transnational reach, rapid dissemination, and weakened guardianship, effects explained through social learning, routine-activity, strain, and online disinhibition theories. Simultaneously, social media furnishes investigators with valuable intelligence, geolocation data, multimedia evidence, and undercover access to networks, but the effective use of these resources is constrained by evidentiary authenticity rules, privacy and data-protection concerns, jurisdictional limits, and uneven institutional capacity within Nigeria's police, EFCC, NITDA, and related agencies. After surveying domestic statutes (notably the Cybercrime Act 2015, Evidence Act 2011, Communications Act 2003, ACJA, and the Terrorism Act 2022) and relevant international instruments, the paper recommends stronger data-protection enforcement, clear admissibility standards for digital evidence, judicial oversight of surveillance, enhanced investigator training and forensic capacity, and improved international cooperation to balance public safety with constitutional rights. These reforms aim to align investigative practice with legal safeguards while mitigating social media's criminogenic effects.*

**Keywords:** Digital, foot prints, Criminal liability Investigation, Legal, Criminological Perspective.

---

\* Dept of Jurisprudence and Public Law, Kwara State University, Malete. 08036949850 Email: Bilikis.Ahmad@Kwasu.Edu.Ng Ayinlaahmadb@Gmail.Com.Orcid 0009-0008-0908-6388

\*\* Final year Law student, Faculty of law, Kwara State University, Malete.

## 1.00 Introduction

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 the law enforcement agents. Though the platforms were designed for social interaction and connection, they have become a double edged sword, creating new avenues for criminal behavior while simultaneously providing law enforcement with unprecedented resources. Platforms such as Facebook, Instagram, Twitter (X), and TikTok have created new digital environments where individual interact, share information, and form virtual communities. While these platforms offer numerous social and economic benefits, they have also created opportunities for criminal behaviour and have reshaped methods of criminal investigation. The intersection between social media, criminal activity, and law enforcement presents complex legal and criminology challenges that require critical examination. Social media has been increasingly linked to various forms of criminal behavior.<sup>1</sup> The anonymity and accessibility provided by these platforms allow offenders to operate with reduced risk of immediate detection, facilitating the expansion of criminal networks and illegal activities across borders<sup>2</sup>. Furthermore, social learning theory suggests that online environments may reinforce deviant behaviour by enabling individuals to observe, imitate, and normalize criminal conduct within digital communities.<sup>3</sup>

At the same time, social media has become an essential investigative tool for law enforcement agencies. Authorities increasingly rely on digital evidence obtained from social networking sites to identify suspects, monitor criminal activities, and gather intelligence.<sup>4</sup> However, the use of social media as an investigative tool raises significant concerns regarding privacy rights, data protection, surveillance, and admissibility of digital evidence in court proceedings.<sup>5</sup>

From a legal perspective, the paper analyzes the challenges posed by digital evidence, jurisdictional issues, and the tension between privacy rights and the imperative for effective law

---

<sup>1</sup> A. Adeoye, —Social Media and the Transformation of Criminal Behaviour in Nigeria,|| *Nigerian Journal of Criminology* (2022) 15 JNL-CRIM 45–62.

<sup>2</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

<sup>3</sup> Akers, R.L., & Jennings, W.G. (2016). *Social Learning Theory*. Routledge.

<sup>4</sup> United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive Study on Cybercrime*.

<sup>5</sup> Taylor, M., Fritsch, E., Liederbach, J., & Holt, T. (2019). *Digital Crime and Digital Terrorism*. Pearson.

enforcement.<sup>6</sup> Scholars have documented the explosion of internet-mediated offences, the lack of adequate technical capacity among investigators, and the weak regulatory framework for handling cybercrime and digital evidence.<sup>7</sup> Yet there remains limited systematic analysis of how social-media evidence is actually treated in Nigerian criminal proceedings, and how existing legal rules interact with investigative practice on the ground.<sup>8</sup>

This paper, therefore, examines the dual role of social media as both a facilitator of criminal behaviour and a key investigative tool, with a focus on the legal and criminological challenges this creates for the Nigerian criminal-justice system. It analyses how social media influences offending patterns, how law-enforcement agencies use digital evidence from these platforms, and how extant legal frameworks struggle to balance public safety, privacy, and due-process rights.<sup>9</sup> By situating the Nigerian experience within broader global debates, the study aims to clarify gaps in doctrine and practice and to suggest concrete improvements to law, policy, and investigative technique in the digital age.<sup>10</sup>

## 2.00 Legal Framework

The increasing use of social media has significantly influenced criminal behaviour and criminal investigations. As a result, several legal frameworks have been established to regulate online activities, criminalize cyber-related offences, and guide law enforcement agencies in investigating crimes committed through digital platforms. In Nigeria, these frameworks consist of constitutional provisions, statutory laws, and institutional regulations that govern the use of digital technologies and social media.

---

<sup>6</sup> Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*.

<sup>7</sup> O. Onyishi, —Challenges of Cybercrime Prosecution in Nigeria,|| Nigerian Journal of Legal Practice (2021) 12 NJLP 78–94.

<sup>8</sup> P. I. O. Nwogu, —Digital Evidence and the Nigerian Criminal Justice System,|| Nigerian Journal of Law and Technology (2023) 5 NJLT 33–50.

<sup>9</sup> G. A. Adebayo, —Privacy, Surveillance and Social Media in Nigeria,|| Journal of Law, Information and Technology (2022) 14 J-LIT 201–218.

<sup>10</sup> S. O. Afolabi, —Reforming the Legal Framework for Cybercrime in Nigeria,|| Nigerian Journal of Public Law (2024) 17 NJPL 1–22.

The rapid growth of social media has significantly transformed communication, commerce, and professional practices in Nigeria. However, this development has also increased the prevalence of cybercrimes such as identity theft, cyberstalking, online fraud, defamation, and other forms of digital misconduct. Consequently, Nigeria has developed a legal framework to regulate online activities and address cybercrime facilitated through social media platforms.

**2.1 The Cybercrime (Prohibition, Prevention, etc.) Act<sup>11</sup>:** This is the primary legislation governing cyber activities in Nigeria. It is a key Nigerian statute enacted to provide a unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes in Nigeria. It was signed into law in 2015 in response to the rising tide of cyber-enabled offences, particularly financial fraud, identity theft, online scams, and other digital crimes for which there was previously no comprehensive statutory regime. The Act also seeks to protect critical national information infrastructure, promote cyber security, and safeguard intellectual property and privacy rights in the digital environment. The Act empowers law enforcement agencies to investigate and prosecute cyber offences committed through digital platforms, including social media networks. It also establishes penalties for offenders and provides mechanisms for cooperation with international agencies in tackling cross-border cybercrime. Additionally, the Act mandates cooperation between service providers, financial institutions, and government agencies to assist in the detection and prevention of cybercrime.<sup>12</sup>

**2.2 Evidence Act<sup>13</sup> :** In addition to the Cybercrimes Act, other relevant laws include the **Evidence Act** which provides the general framework for the admissibility, relevance, and evaluation of evidence in Nigerian courts, including emerging forms of digital and electronic evidence. It recognizes the admissibility of electronic evidence in court. It replaced the outdated Evidence Act, Cap. E14, Laws of the Federation of Nigeria, and came into force on 3 June 2011. It was enacted to modernise evidentiary rules, harmonise them across civil and criminal proceedings, and align Nigerian practice with international standards. A key innovation of the Act is its express recognition and treatment of electronic evidence, such as emails, text messages, and digital

---

<sup>11</sup> The Cybercrime (Prohibition, Prevention, etc.) Act, 2015, (No. 17 of 2015) Laws of the Federation of Nigeria (LFN), Cap. C25, 2004 (reprint 2015), as amended.

<sup>12</sup> Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 24.

<sup>13</sup> The Evidence Act 2011,(No 18 of 2011)

records, subject to rules on authenticity and reliability<sup>14</sup>. Social media communications such as messages, posts, images, and videos may serve as evidence during criminal investigations and prosecutions. The Act establishes the conditions under which **computer-generated evidence** may be admitted in court. This provision requires the party presenting the evidence to demonstrate that the computer used to produce the information was operating properly and that the data was generated in the course of regular use. This legal provision has become particularly relevant in criminal investigations involving social media activities such as fraud, threats, and conspiracy conducted through digital platforms.<sup>15</sup>

**2.3 The Nigerian Communications Act<sup>16</sup>:** is the primary statute governing the Nigerian communications sector; it was signed into law by President Olusegun Obasanjo on 8 July 2003 after passage by both Houses of the National Assembly. The Act applies to the provision and use of all communications services and networks operating wholly or partly in Nigeria and establishes the Nigerian Communications Commission (NCC) as an independent regulatory authority. Its objectives include promoting the implementation of national communications policy, ensuring fair competition, protecting consumer and service-provider interests, managing national resources such as spectrum and electronic addresses, and safeguarding national security and safety in the use of communications infrastructure. It establishes the legal and regulatory framework for telecommunications and communications services in Nigeria, including the mandate of the Nigerian Communications Commission (NCC). It also regulates telecommunications service providers and ensures compliance with national communication policies. Together, these laws form a comprehensive legal framework aimed at addressing cybercrime and regulating online activities within Nigeria's digital environment.

---

<sup>14</sup> Section 84 of the Evidence Act 2011

<sup>15</sup> Evidence Act 2011, s 84.

<sup>16</sup> The Nigerian Communications Act 2003 Laws of the Federation of Nigeria (LFN), 2004

**2.4 The Constitution of the Federal Republic of Nigeria 1999<sup>17</sup>:** The Constitution provides the foundational legal framework regulating the right to freedom of expression in Nigeria. It guarantees the right to freedom of expression and the freedom to receive and impart information through any medium, including social media platforms.<sup>18</sup> However, this right is not absolute. It may be restricted in the interest of public safety, national security, and the prevention of crime. These constitutional provisions create a balance between protecting citizens' fundamental rights online and enabling the government to regulate harmful online behavior such as cyber bullying, hate speech, and incitement to violence.<sup>19</sup>

**2.5 Administration of Criminal Justice Act (ACJA)<sup>20</sup>:** It is a federal law enacted to reform and modernise Nigeria's criminal-justice system by promoting efficient case management, timely dispensation of justice, and respect for the rights of suspects, defendants, and victims. It applies to offences established by an Act of the National Assembly and to criminal proceedings in the Federal Capital Territory and other federal courts, and many of its provisions have been adopted or adapted by several states through Administration of Criminal Justice Laws (ACJLs). The Act introduces key safeguards such as time-bound remand procedures, stronger protections against unlawful detention, mandatory disclosure rules, better regulation of plea bargaining, and clearer protocols for witness-protection, evidence-handling, and digital-evidence use in the process. It provides the overarching framework for criminal procedure in the Federal Capital Territory and other federal courts in Nigeria, from arrest to trial, sentencing, and appeals. It also provides procedural safeguards governing criminal investigations and prosecutions in Nigeria. Sections 1, 15, 17, and 37 emphasize due process, proper documentation of arrests and seized property, and the recording of statements, including electronic recordings. These provisions support the lawful acquisition and handling of digital evidence during investigations involving social media.

---

<sup>17</sup> The Constitution of the Federal Republic of Nigeria 1999 as amended

<sup>18</sup> Section 39 1999 Const FRN

<sup>19</sup> Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

<sup>20</sup> The Administration of Criminal Justice Act 2015

## 2.5 Criminal Code Act and Penal Code

The Criminal Code Act<sup>21</sup> and Penal Code<sup>22</sup> contain several provisions that can apply to crimes committed through social media platforms. These include offences such as defamation, conspiracy, fraud, impersonation, and incitement to violence. Although these laws were enacted before the emergence of social media, their provisions have been adapted to address offences committed through digital communication channels.

## 2.6 Nigerian Communications Act 2003

The Nigerian Communications Act regulates telecommunications services and establishes the Nigerian Communications Commission (NCC). The Act provides regulatory oversight over internet service providers and telecommunications operators, which are essential for monitoring and controlling online communications. The Act also allows regulatory authorities to collaborate with security agencies during criminal investigations involving digital communication networks.

## 2.7 Terrorism (Prevention and Prohibition) Act 2022

Social media platforms are sometimes used to promote extremist ideologies, recruit members, and coordinate criminal activities. The **Terrorism (Prevention and Prohibition) Act 2022** criminalizes the use of communication platforms, including social media, for acts related to terrorism. The Act authorizes security agencies to monitor communications suspected to be linked with terrorist activities and prosecute individuals who disseminate terrorist propaganda online.<sup>23</sup>

## 2.8 International Legal Framework

Since social media crimes often cross national boundaries, international cooperation is necessary. Various international instruments such as the Council of Europe Convention on Cybercrime and other global cybersecurity initiatives provide guidelines for combating transnational cyber offences. These frameworks encourage cooperation between countries in areas such as extradition, information sharing, and digital evidence collection. Handling of social media-related crime and digital evidence is shaped by a constellation of treaties, guidelines, and technical standards aimed

---

<sup>21</sup> Sections 373, 375, 516, 419 and 484 Criminal code

<sup>22</sup> Sections 391, 392, 322, 96 and 114 Penal Code.

<sup>23</sup> Terrorism (Prevention and Prohibition) Act 2022, ss 13–18.

at promoting cooperation, harmonising evidentiary practices, and protecting human rights.<sup>24</sup> Key instruments include the United Nations Convention against Transnational Organized Crime (UNTOC, 2000) and the United Nations Convention against Corruption (UNCAC, 2003), which encourage States to cooperate in obtaining and sharing evidence in cross-border investigations, including electronic data generated on social-media platforms. The Council of Europe's Budapest Convention on Cybercrime (2001) further provides a widely adopted regional framework on substantive cybercrime offences and procedures for rapid mutual-legal assistance in the production of digital evidence, influencing many national laws on cybercrime and digital-evidence handling. International bodies such as the United Nations Office on Drugs and Crime (UNODC) have developed practical tools such as the handbook on electronic evidence and the Global Initiative on Handling Electronic Evidence, which guide States on how to obtain and use electronic evidence across borders while respecting privacy and fair-trial standards. UNESCO and other organisations have issued guidelines for prosecutors on collecting digital evidence in ways compatible with international standards on freedom of expression and privacy, thereby setting benchmarks for how social-media data may be used in criminal investigations and at trial. Together, these international instruments and guidelines form a normative framework against which Nigeria's own laws such as the Cybercrime (Prohibition, Prevention, etc.) Act 2015 and the Evidence Act 2011 can be assessed in the context of social media-driven criminal behaviour and investigation.<sup>25</sup>

## **2.9 Institutional Framework for Cybercrime Investigation**

Apart from statutory laws, several institutions play important roles in investigating social media-related crimes. These include: The Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices Commission (ICPC), National Information Technology Development Agency (NITDA).<sup>26</sup> These agencies collaborate to detect, investigate, and prosecute crimes facilitated through digital platforms. The effectiveness of these institutions is

---

<sup>24</sup> United Nations, *Convention against Transnational Organized Crime, 2000*, General Assembly Resolution 55/25, UN Doc. A/RES/55/25.

<sup>25</sup> United Nations, *Convention against Corruption, 2003*, General Assembly Resolution 58/4, UN Doc. A/RES/58/4.

<sup>26</sup> Daudu S.O. and Idehen S.O., 'Legal and Institutional Framework for Combating Cybercrimes in Nigeria' (2024) 1(1) *LexScriptio: A Journal of Jurisprudence and Public Law* 251.

essential because cybercrime investigation involves digital forensics, intelligence gathering, and lawful interception of communication data.

The Nigerian Communications Commission (NCC) is responsible for overseeing the telecommunications sector and facilitating cooperation between service providers and law-enforcement agencies in the production of digital evidence, while the Economic and Financial Crimes Commission (EFCC) and the National Cybercrime Centre (NCCC) handle the investigation and prosecution of complex cyber-offences and financial-crime-linked cyber-activities. The police and other security-service units also participate in cybercrime investigations, often through specialised cyber-crime squads or digital-forensics units, though their capacity and coordination remain uneven.

At the international level, the institutional response to cybercrime is coordinated through multilateral bodies such as the United Nations Office on Drugs and Crime (UNODC), Interpol, and the Council of Europe, which encourage States to establish or strengthen national cyber-crime units, forensic-investigation teams, and joint-task-force arrangements. These organisations emphasise the importance of inter-agency collaboration, public-private partnerships with internet and telecommunications providers, and standardised training frameworks for cyber-crime investigators to ensure that digital evidence is collected and preserved in a manner consistent with rule-of-law and human-rights standards. Nigeria's institutional architecture reflects this global model but still faces challenges in harmonising mandates, allocating adequate technical and financial resources, and building sustainable investigative capacity across agencies.

### **3.00 Social Media as a Facilitator of Criminal Behaviour**

The emergence and widespread use of social media platforms have significantly influenced patterns of criminal behaviour in modern society. Social media has transformed communication by enabling individuals to interact, share information, and create virtual communities without geographical limitations. While these platforms offer social, educational, and economic benefits, they have also created opportunities for criminal activities to develop and expand. The accessibility, anonymity, and rapid communication features of social media have contributed to the evolution of criminal strategies and have made criminal behaviour more complex and

difficult to regulate.<sup>27</sup>This often results in severe psychological harm to victims, including depression, anxiety, and in extreme cases, self-harm or suicide.<sup>28</sup>

Social media has also facilitated financial crimes such as fraud and identity theft. Criminals frequently use social networking platforms to create fake profiles, impersonate legitimate organizations, or conduct phishing schemes to obtain personal and financial information from unsuspecting users. The large amount of personal data shared on social media platforms makes individuals vulnerable to exploitation. Criminals may use stolen identities to commit further offences, including financial fraud, online scams, and unauthorized transactions.<sup>29</sup>

Another major concern is the use of social media to promote hate speech, extremist ideologies, and radicalization. Online platforms provide a space where extremist groups can disseminate propaganda, recruit new members, and coordinate criminal activities. The global reach of social media allows these groups to influence individuals across different countries and cultural backgrounds. Research indicates that exposure to extremist content online may contribute to the normalization of violent beliefs and encourage individuals to participate in criminal or terrorist activities.<sup>30</sup>

Organized criminal groups increasingly rely on social media to facilitate illegal operations such as human trafficking, drug trafficking, and illegal arms trading. Social media provides criminals with a convenient and cost-effective method of advertising illegal services, communicating with clients, and coordinating criminal networks. The ability to operate across multiple jurisdictions makes it difficult for law enforcement agencies to detect and prevent these activities. The use of encrypted messaging and anonymous online transactions further complicates criminal investigations.<sup>31</sup>

---

<sup>27</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

<sup>28</sup> Hinduja, S., & Patchin, J.W. (2018). *Cyberbullying: Identification, Prevention and Response*. Cyberbullying Research Center.

<sup>29</sup> Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society*. Sage Publications.

<sup>30</sup> Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA).

<sup>31</sup> United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.

Several characteristics of social media contribute to its role in facilitating criminal behaviour. Anonymity is one of the most significant factors, as it allows individuals to hide their real identities through fake accounts or pseudonyms. This reduces accountability and increases the likelihood of engaging in illegal activities. Additionally, the accessibility and global connectivity of social media platforms enable offenders to target victims from different geographical locations. This transnational nature of social media crime presents challenges for law enforcement agencies due to differences in legal systems and regulatory frameworks across countries.<sup>32</sup>

Criminological theories provide valuable explanations for how social media influences criminal behaviour. Social learning theory suggests that individuals learn behaviour through observation and interaction with others. Social media exposes users to deviant behaviour, which may encourage imitation and reinforcement of criminal activities within online communities. Individuals who frequently engage with online groups that support illegal behaviour may develop attitudes that justify or normalize criminal conduct.<sup>33</sup>

This psychological effect increases the likelihood of cyberbullying, harassment, and other forms of online deviance.<sup>34</sup> Similarly, routine activity theory explains how social media creates virtual environments where motivated offenders encounter suitable targets in the absence of effective guardianship, thereby increasing the risk of criminal activity.<sup>35</sup>

### **3.1 Types of Crimes Associated with Social Media**

Understanding the types of crimes associated with social media is critical for criminologists, legal practitioners, and law enforcement agencies seeking to develop effective prevention and intervention strategies. Recognizing the types of crimes associated with social media is essential for developing effective policies, investigative strategies, and preventive interventions.

---

<sup>32</sup> Holt, T.J. (2017). *Crime Online: Correlates, Causes and Context*. Carolina Academic Press.

<sup>33</sup> Akers, R.L., & Jennings, W.G. (2016). *Social Learning Theory*. Routledge.

<sup>34</sup> Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), 321–326.

<sup>35</sup> Cohen, L.E., & Felson, M. (1979). Social Change and Crime Rate Trends. *American Sociological Review*, 44(4), 588–608.

### 3.1.1 Cyberbullying and Online Harassment

One of the most prevalent types of crime associated with social media is cyberbullying. This involves the use of digital platforms to threaten, intimidate, or humiliate individuals. Victims may experience emotional distress, depression, and anxiety as a result of persistent online abuse. Social media amplifies the reach of cyberbullying, allowing harmful messages or media to spread rapidly to large audiences.<sup>36</sup> Online harassment can occur in personal contexts, workplaces, or school environments, and often involves the repeated targeting of victims by individuals or groups.<sup>37</sup>

### 3.1.2 Identity Theft and Fraud

Social media has facilitated the rise of identity theft and online fraud. Criminals exploit personal information shared on platforms to impersonate individuals or organizations. Techniques such as phishing, fake profiles, and social engineering are commonly used to gain access to financial accounts, confidential data, or sensitive personal information.<sup>38</sup> Identity theft on social media can lead to significant financial loss, reputational damage, and long-term legal complications for victims.<sup>39</sup>

### 3.1.3 Hate Speech and Extremist Activities

The proliferation of hate speech and extremist content is another major concern linked to social media. Platforms can be used to propagate racist, sexist, or otherwise discriminatory ideologies, sometimes escalating to incitement of violence.<sup>40</sup> Extremist groups also utilize social media to recruit members, disseminate propaganda, and coordinate criminal activities. These crimes often

---

<sup>36</sup> Hinduja, S., & Patchin, J.W. (2018). *Cyberbullying: Identification, Prevention and Response*. Cyberbullying Research Center.

<sup>37</sup> Livingstone, S., & Haddon, L. (2018). *Children, Risk and Safety on the Internet*. Policy Press.

<sup>38</sup> Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society*. Sage Publications.

<sup>39</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

<sup>40</sup> Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*.

have a transnational dimension, posing significant challenges for law enforcement agencies due to jurisdictional and cultural differences.<sup>41</sup>

### **3.1.4 Cyberstalking**

involves the repeated use of social media or other digital platforms to harass or threaten an individual. Offenders may monitor victims' online activity, send threatening messages, or post private information without consent.<sup>42</sup> Social media's accessibility and real-time updates increase the potential for cyberstalking, as offenders can track victims' movements, relationships, and online behaviour. This form of crime can escalate into physical stalking or violence if unchecked.<sup>43</sup>

### **3.1.5 Sexual Exploitation and Online Grooming**

Social media has been used to facilitate sexual exploitation, including child grooming and the distribution of sexually explicit material. Offenders often engage with minors through private messaging, online games, or social networking sites to build trust and manipulate them for sexual purposes.<sup>44</sup> The anonymity and privacy features of social media make detection and prevention difficult, while the permanence of digital content increases the potential harm to victims.<sup>45</sup>

### **3.1.6 Financial Crimes and Scams**

Financial crimes such as online scams, investment fraud, and cryptocurrency fraud have been increasingly associated with social media platforms. Criminals create fake business accounts, fraudulent advertisements, or misleading promotions to deceive users and solicit money or

---

<sup>41</sup> United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.

<sup>42</sup> Holt, T.J. (2017). *Crime Online: Correlates, Causes and Context*. Carolina Academic Press.

<sup>43</sup> Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

<sup>44</sup> Wolak, J., Finkelhor, D., & Mitchell, K.J. (2012). Child Pornography Possessors: Trends in Offender and Case Characteristics. *Sexual Abuse*, 24(4), 313–332.

<sup>45</sup> Casey, E. (2011). *Digital Evidence and Computer Crime*. Academic Press.

sensitive information.<sup>46</sup> Social media's rapid dissemination of information and viral content increases the reach and effectiveness of these scams, often affecting large numbers of unsuspecting users.<sup>47</sup>

### **3.1.7 Organized Crime and Coordination of Illegal Activities**

Organized criminal groups utilize social media to coordinate illegal activities, including drug trafficking, human trafficking, and illegal arms sales.<sup>48</sup> These platforms allow criminals to communicate quickly, advertise services, and recruit new members across different countries. The transnational nature of social media crime complicates law enforcement investigations due to varying legal frameworks and the anonymity of online interactions.<sup>49</sup>

### **3.1.8 Misinformation, Fake News, and Cyberterrorism**

Social media also plays a role in the spread of misinformation, fake news, and cyberterrorist activities. Criminals can exploit platforms to manipulate public opinion, create panic, or incite violence. These activities may indirectly facilitate criminal behaviour, such as riots, scams, or politically motivated attacks, by influencing large groups of people through coordinated digital campaigns.<sup>50</sup>

## **4.00 Features of Social media that Enable Crime**

Social media platforms, while designed primarily for communication, information sharing, and social interaction, possess inherent features that can inadvertently facilitate criminal behaviour. The technological and structural characteristics of these platforms create opportunities for offenders to engage in illegal activities, often with minimal risk of detection or immediate

---

<sup>46</sup> Holt, T.J., & Bossler, A.M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

<sup>47</sup> Goldsmith, A., & Brewer, R. (2015). *Digital Policing*. Routledge

<sup>48</sup> Taylor, M., Fritsch, E., Liederbach, J., & Holt, T. (2019). *Digital Crime and Digital Terrorism*. Pearson.

<sup>49</sup> Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

<sup>50</sup> Yar, M. (2013). *Cybercrime and Society*. Sage Publications.

consequence. Understanding these features is essential for developing effective preventive and investigative strategies.

#### **4.1 Anonymity and Pseudonymity**

One of the most significant enablers of online crime is the ability of users to remain anonymous or use pseudonyms.<sup>51</sup> Social media platforms allow individuals to create accounts without providing verifiable personal information, making it easier for offenders to conceal their identities. Research indicates that online anonymity is strongly linked to increased aggressive and deviant behaviours because users feel less accountable for their actions.<sup>52</sup>

#### **4.2 Accessibility and Convenience**

Social media platforms are highly accessible, allowing users to connect from any location at any time.<sup>53</sup> The convenience of social media also allows for rapid dissemination of criminal content.<sup>54</sup>

#### **4.3 Global Reach and Transnational Interaction**

Social media enables users to communicate across geographic boundaries instantly. While this global connectivity offers numerous benefits,<sup>55</sup> the global reach of social media complicates law enforcement responses due to jurisdictional challenges and differences in international legal frameworks.<sup>56</sup>

#### **4.4 Rapid Information Dissemination**

Platforms such as X (formerly Twitter), TikTok, and Facebook allow for the instant sharing of text, images, videos, and links. This rapid information flow can be exploited by criminals to

---

<sup>51</sup> Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), 321–326.

<sup>52</sup> Akers, R.L., & Jennings, W.G. (2016). *Social Learning Theory*. Routledge.

<sup>53</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

<sup>54</sup> Holt, T.J. (2017). *Crime Online: Correlates, Causes and Context*. Carolina Academic Press.

<sup>55</sup> United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.

<sup>56</sup> Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.

spread illegal content, misinformation, or instructions for committing crimes.<sup>57</sup> The speed and viral nature of social media content can amplify the effects of criminal acts, such as the rapid propagation of hate speech, extremist material, or coordinated fraud schemes.<sup>58</sup>

#### **4.5 Lack of Effective Guardianship**

Routine activity theory suggests that crime is more likely to occur when capable guardians are absent. On social media, oversight mechanisms are often inadequate to monitor all interactions in real time. While platforms implement content moderation and reporting tools, the sheer volume of posts and messages makes it impossible to prevent all criminal activity. This lack of effective supervision provides offenders with opportunities to exploit vulnerable users, conduct scams, or engage in harassment without immediate intervention.<sup>59</sup>

#### **4.6 Permanence and Traceability of Content**

Content posted on social media can remain accessible for long periods, sometimes indefinitely. While this permanence can serve as a tool for investigators, it also allows offenders to create a persistent digital footprint that can facilitate repeated victimization. Criminals may use historical posts, shared media, or profile information to plan targeted attacks, harass victims over time, or manipulate online interactions.<sup>60</sup>

#### **4.7 Peer Influence and Community Norms**

Social media platforms enable the formation of online communities and peer networks. While these communities can be positive, they can also normalize deviant behaviour and create environments where criminal conduct is encouraged or rewarded. For example, groups promoting cybercrime techniques, illegal financial schemes, or extremist ideologies can

---

<sup>57</sup> Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society*. Sage Publications.

<sup>58</sup> Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA)*.

<sup>59</sup> Cohen, L.E., & Felson, M. (1979). Social Change and Crime Rate Trends. *American Sociological Review*, 44(4), 588–608.

<sup>60</sup> Casey, E. (2011). *Digital Evidence and Computer Crime*. Academic Press.

influence members to participate in illegal activities, reinforcing deviant norms through online interactions.<sup>61</sup>

#### **4.8 Integration with Third-Party Applications**

Many social media platforms integrate with third-party apps, games, and services, which may access personal information and communication networks. These integrations can inadvertently provide criminals with additional vectors for exploiting user data or conducting fraud. Offenders can use vulnerabilities in connected apps to harvest data, send malicious links, or gain unauthorized access to accounts.<sup>62</sup>

### **5.00 Criminological Explanations of Social Media Crime**

Understanding the impact of social media on criminal behaviour requires the application of established criminological theories, which offer insights into why individuals engage in online criminal activities and how digital environments influence deviant conduct. Social media not only facilitates opportunities for crime but also shapes behavioural patterns through social interaction, observation, and environmental factors.

**5.1 Social Learning Theory** posits that criminal behaviour is learned through observation, imitation, and reinforcement within social contexts.<sup>63</sup> On social media, individuals are exposed to deviant behaviours and repeatedly observe peers engaging in illegal or unethical activities without immediate consequences, they may be encouraged to adopt similar behaviours. Social media communities can therefore act as virtual —learning environments‖ where deviant norms are reinforced.<sup>64</sup>

**5.2 The Online Disinhibition Effect**, proposed by Suler, provides a psychological perspective on why individuals behave differently online than offline. The perceived anonymity, invisibility,

---

<sup>61</sup> Akers, R.L., & Jennings, W.G. (2016). *Social Learning Theory*. Routledge.

<sup>62</sup> Holt, T.J., & Bossler, A.M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

<sup>63</sup> Akers, R.L., & Jennings, W.G. (2016). *Social Learning Theory*. Routledge.

<sup>64</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

and lack of immediate accountability on social media platforms reduce inhibitions, making users more likely to engage in aggressive, antisocial, or criminal conduct.<sup>65</sup> This theory helps explain the prevalence of cyberbullying, online harassment, and hate speech, where individuals act in ways they would not in face-to-face interactions.<sup>66</sup>

**5.3 Routine Activity Theory** offers another lens for understanding social media-facilitated crime. The theory suggests that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship. Social media platforms, by creating constant and widespread digital interaction, provide motivated offenders with easy access to potential victims while offering limited oversight or monitoring. For example, oversharing personal information on social media can make individuals more vulnerable to identity theft, fraud, or online stalking.<sup>67</sup>

**5.4 Strain Theory** provides insights into how social media may exacerbate criminal behaviour by creating pressures and frustrations that lead individuals to deviate. Social comparison on social networking sites can generate feelings of inadequacy, envy, or exclusion, which may motivate some individuals to engage in deviant behaviour as a coping mechanism, including hacking, cyber fraud, or online harassment.<sup>68</sup>

**5.5 Control Theory** highlights the role of social bonds in preventing crime. Social media can weaken traditional social controls by encouraging interactions within deviant or criminally inclined online communities. When individuals are more strongly influenced by digital peer groups than by family, school, or community norms, the likelihood of engaging in criminal activity increases.<sup>69</sup>

---

<sup>65</sup> Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), 321–326.

<sup>66</sup> Holt, T.J. (2017). *Crime Online: Correlates, Causes and Context*. Carolina Academic Press.

<sup>67</sup> Cohen, L.E., & Felson, M. (1979). Social Change and Crime Rate Trends. *American Sociological Review*, 44(4), 588–608.

<sup>68</sup> Merton, R.K. (1938). Social Structure and Anomie. *American Sociological Review*, 3(5), 672–682.

<sup>69</sup> Hirschi, T. (1969). *Causes of Delinquency*. University of California Press.

Incorporating these criminological perspectives provides a multi dimensional understanding of social media related crime. It emphasizes that criminal behaviour in digital contexts is influenced not only by technological affordances but also by social, psychological, and environmental factors.<sup>70</sup>

### **6.00 Social Media as a Tool in Criminal Investigations**

One of the most significant uses of social media in criminal investigations is intelligence gathering. Law enforcement agencies monitor social media platforms to identify suspects, track criminal networks, and detect potential criminal activities before they occur. Criminals frequently use social media to communicate, share information, and coordinate illegal activities, often leaving digital footprints that investigators can analyse. Publicly shared posts, images, videos, and comments often provide valuable insights into criminal behaviour, relationships between suspects, and potential evidence linking individuals to criminal acts.<sup>71</sup>

Social media has also enhanced surveillance and undercover investigation techniques. Investigators may create undercover profiles or monitor existing online communities to gain access to criminal networks. This approach is particularly useful in investigating organized crime, gang-related activities, and terrorism. Social media surveillance allows law enforcement agencies to monitor communication patterns and identify individuals involved in illegal activities without immediate physical interaction. Such investigative methods have proven effective in preventing criminal acts and dismantling criminal organizations.<sup>72</sup>

Another important role of social media in criminal investigations is the collection of digital evidence. Social media platforms contain a wide range of information, including private messages, multimedia content, geolocation data, and online transaction records. Investigators use digital forensic techniques to collect, preserve, and analyse this information to support criminal cases. Digital evidence obtained from social media has been used in cases involving fraud,

---

<sup>70</sup> Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society*. Sage Publications.

<sup>71</sup> Goldsmith, A., & Brewer, R. (2015). *Digital Policing*. Routledge.

<sup>72</sup> Taylor, M., Fritsch, E., Liederbach, J., & Holt, T. (2019). *Digital Crime and Digital Terrorism*. Pearson.

cybercrime, assault, and even homicide. For example, photographs or videos posted by suspects may provide evidence of their presence at crime scenes or involvement in illegal activities.<sup>73</sup>

Geolocation data available through social media platforms has become a valuable investigative tool. Many social media users share location-based information when posting content, which can help investigators track suspects' movements and establish timelines for criminal activities. Metadata embedded in social media posts, such as timestamps and device information, can further strengthen the reliability of digital evidence. These technological advancements have improved the efficiency and accuracy of criminal investigations.<sup>74</sup>

#### **7.00 Legal and Ethical Challenges to the effect of social media on criminal behavior and investigation**

The increasing rate of cybercrimes facilitated through social media platforms has created enforcement challenges for Nigerian authorities. Nwocha, Iteshi, and Awada note that while the legal framework exists, enforcement agencies often face difficulties such as jurisdictional issues, digital evidence management, and technological limitations.<sup>75</sup>

Social media has increasingly become a tool for both legitimate legal practice and criminal activities. According to Omoleke, social media platforms are now widely used by legal practitioners for communication, legal awareness campaigns, and professional networking, although the unregulated use of these platforms raises concerns about professional ethics and confidentiality.<sup>76</sup>

**7.1 Privacy and Data Protection Issues** The increasing reliance on social media in criminal behaviour and criminal investigations has created significant legal and ethical challenges for modern criminal justice systems. While social media platforms provide valuable tools for communication, information sharing, and law enforcement investigations, its use raises concerns

---

<sup>73</sup> Casey, E. (2011). *Digital Evidence and Computer Crime*. Academic Press.

<sup>74</sup> Holt, T.J. (2017). *Crime Online: Correlates, Causes and Context*. Carolina Academic Press.

<sup>75</sup> Nwocha M.E., Iteshi C.V. and Awada P.M., 'Social Media Facilitated Cybercrimes in Nigeria and the Challenges of Legal Enforcement' (2024) 5(3) *Law and Social Justice Review*.

<sup>76</sup> Omoleke O., 'The Role of Social Media in Legal Practice in Nigeria' (2025) *ABUAD Law Journal*.

regarding privacy rights, data protection, freedom of expression, and the ethical limits of surveillance.<sup>77</sup>

7.2 Conflict With Constitutional and Human Rights Protections that safeguard individuals from unlawful surveillance and intrusion into private life. Balancing the need for public safety with the protection of individual privacy remains a major concern for legal systems worldwide.<sup>78</sup>

7.3 Courts require digital evidence to meet strict standards of authenticity, reliability, and relevance before it can be accepted. Establishing ownership and authorship of social media content is often challenging due to the anonymity and potential manipulation of online information. The presence of fake accounts, altered digital content, and technological vulnerabilities may undermine the credibility of social media evidence and complicate judicial processes.<sup>79</sup>

7.4 Challenges of Jurisdictional limitations further complicate the regulation of social media-related crime. Social media platforms operate globally, allowing criminal activities to occur across national borders. Differences in legal systems, data protection laws, and enforcement procedures make it difficult for law enforcement agencies to investigate and prosecute transnational cybercrime effectively.<sup>80</sup>

7.5 Ethical principles require that social media monitoring be conducted in a transparent, proportionate, and accountable manner to prevent abuse of power and protect democratic values.<sup>81</sup>

7.6 Balancing Public Safety and Individual Rights Privacy concerns are among the most significant issues associated with social media surveillance. Monitoring online activities may conflict with individuals' rights to privacy and freedom of expression.<sup>82</sup>

---

<sup>77</sup> Wall, D.S. (2015). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

<sup>78</sup> Solove, D.J. (2021). *Understanding Privacy*. Harvard University Press.

<sup>79</sup> Mason, S. (2017). *Electronic Evidence*. Institute of Advanced Legal Studies.

<sup>80</sup> Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger

<sup>81</sup> Richards, N.M. (2015). *The Dangers of Surveillance*. Harvard University Press.

<sup>82</sup> Solove, D.J. (2021). *Understanding Privacy*. Harvard University Press.

7.7 Need for Policy and Investigative Improvements investigators must maintain a proper chain of custody to ensure that digital evidence is not altered or tampered with during the investigation process.<sup>83</sup>

7.8 Enhancing Investigative Techniques The effectiveness of social media as an investigative tool depends largely on technological advancements and the training of law enforcement personnel. Investigators must possess specialized skills in digital forensics, data analysis, and cybercrime detection to effectively utilise social media evidence.<sup>84</sup>

## **8.00 Recommendations**

Umejiaku and Uzoka highlight that social media related cybercrimes in Nigeria range from impersonation and online fraud to harassment and cyberbullying. They emphasize the need for effective legal remedies, stronger institutional capacity, and public awareness to ensure that victims can obtain adequate protection and justice under the law.<sup>85</sup> In light of the numerous legal, ethical, and investigative challenges associated with the use of social media in criminal behaviour and investigations, several measures should be adopted to strengthen the regulatory and investigative framework.

### **8.1 Strengthening Data Protection and Privacy Regulations**

To address data protection concerns arising from social media surveillance, the Nigerian government should strengthen existing data protection laws and ensure strict compliance with privacy standards. The implementation of robust data protection policies will help regulate how law enforcement agencies collect, store, and utilize personal information obtained from social media platforms.

In addition, regulatory authorities such as the National Information Technology Development Agency (NITDA) should ensure effective enforcement of the Nigeria Data Protection Act to safeguard citizens against misuse of their personal data during criminal investigations.

---

<sup>83</sup> Mason, S. (2017). *Electronic Evidence*. Institute of Advanced Legal Studies.

<sup>84</sup> INTERPOL. (2021). *Global Cybercrime Strategy*

<sup>85</sup> Umejiaku N.O. and Uzoka N.C., ‘An Overview of Social Media Related Cybercrimes and its Legal Remedy’ (2021) 2(2) *Law and Social Justice Review*.

## **8.2 Ensuring Compliance with Constitutional and Human Rights Standards**

Law enforcement agencies must ensure that the use of social media monitoring tools does not violate constitutional rights, particularly the right to privacy and freedom of expression guaranteed under the Constitution of the Federal Republic of Nigeria 1999 (as amended).

Investigative authorities should obtain proper judicial authorization before conducting digital surveillance or accessing private social media communications. This will ensure that investigations are conducted within the limits of the law and in compliance with internationally recognized human rights principles.

## **8.3 Establishing Clear Standards for Admissibility of Digital Evidence**

Courts and law enforcement agencies should develop clear guidelines governing the collection, authentication, and admissibility of social media evidence. Digital forensic experts should be engaged to verify the authenticity of social media content presented in court. Furthermore, the judiciary should adopt standardized procedures for verifying authorship and ownership of social media accounts in order to minimize the risks associated with fake accounts and manipulated digital content.

## **8.4 Enhancing International Cooperation to Address Jurisdictional Challenges**

Social media crimes often transcend national borders, Nigeria should strengthen international cooperation mechanisms to combat transnational cybercrime effectively. This may include entering into bilateral and multilateral agreements with other countries for information sharing, mutual legal assistance, and extradition of cybercrime offenders. Such cooperation will enable law enforcement agencies to obtain digital evidence stored on foreign servers and prosecute offenders operating across multiple jurisdictions.

## **8.5 Promoting Ethical Guidelines for Social Media Surveillance**

Government agencies responsible for criminal investigations should adopt clear ethical guidelines governing the monitoring of social media activities. These guidelines should emphasize transparency, accountability, and proportionality in surveillance practices. Independent oversight bodies should also be established to monitor the activities of law enforcement agencies and ensure that social media surveillance powers are not abused.

### **8.6 Balancing Public Safety with Individual Rights**

Legal frameworks regulating social media investigations should strike an appropriate balance between ensuring public safety and protecting individual rights. While it is important for authorities to monitor online activities that threaten national security or public order, such monitoring must not lead to unnecessary intrusion into citizens' private lives. Judicial oversight and legislative safeguards should therefore be strengthened to prevent excessive surveillance.

### **8.7 Improving Policies on Digital Evidence Management**

Law enforcement agencies must implement proper procedures for handling digital evidence obtained from social media platforms. Investigators should maintain a clear chain of custody to ensure that evidence is preserved in its original form and is not altered during the investigation process. Developing standardized protocols for digital evidence management will improve the credibility of social media evidence in criminal proceedings.

### **8.8 Enhancing Investigative Capacity and Technological Expertise**

The effectiveness of social media investigations largely depends on the technical capacity of law enforcement personnel. Therefore, specialized training programs should be organized for investigators in areas such as digital forensics, cyber intelligence, data analysis, and cybercrime investigation techniques. Government agencies should also invest in modern forensic technologies and digital investigation tools to enhance the ability of law enforcement agencies to detect and investigate crimes committed through social media platforms.

## **9.00 Conclusion**

Social media has significantly influenced criminal behaviour and criminal investigation methods in modern society. While these platforms provide opportunities for criminal activities, they also serve as valuable investigative tools for law enforcement agencies. Legal and criminological perspectives highlight the need for updated regulatory measures, improved investigative techniques, and increased public awareness. Addressing the challenges posed by social media requires collaboration between governments, law enforcement agencies, social media companies, and the public to ensure effective crime prevention and protection of individual rights. Implementing the above recommendations will go a long way to curb the vices associated with the use of social media.