

Assessing The Impact of Social Media on Youth Involvement in Criminal Activities in Nigeria

GBENEMENE KPAE

Department of Sociology University of Port Harcourt

Abstract- The proliferation of social media platforms across Nigeria has fundamentally altered the landscape of youth interaction, presenting what many scholars now characterize as a double-edged sword. While these digital spaces offer unprecedented opportunities for connection, learning, and economic empowerment, mounting evidence suggests they may simultaneously function as vectors for criminal socialization among young Nigerians. This article examines the relationship between social media engagement and youth involvement in criminal activities, drawing on secondary data from national reports, academic studies, and institutional surveys published between 2020 and 2025. The study adopts a mixed-methods secondary analysis approach, synthesizing quantitative data from sources including the Nigerian Communications Commission's 2025 Child Online Safety Report, Gatefield's State of Online Harms 2025 report, and multiple peer-reviewed studies conducted across Nigerian universities. Findings indicate that approximately 68.9 million Nigerian internet users, representing half of the country's online population, regularly experience online harms, with youth aged 18–35 constituting the most vulnerable demographic. The research identifies several mechanisms through which social media facilitates criminal involvement: normalization of deviant behaviour through peer networks, dissemination of technical knowledge for cybercrimes, exposure to fraudulent schemes, and recruitment into criminal enterprises. X (formerly Twitter) accounts for 34% of reported online harms, while Facebook and WhatsApp follow closely behind. Theoretically, the article integrates Routine Activity Theory and Social Learning Theory to explain how social media platforms create converging conditions for offending behaviour. The study concludes that current legal frameworks, including the Cybercrime Act, remain insufficient to address the nuanced ways social media shapes youth criminality. Recommendations include enhanced digital literacy curricula, strengthened platform accountability mechanisms, and the urgent passage of comprehensive child online protection legislation.

Keywords: Social Media, Youth Criminality, Cybercrime, Nigeria, Online Harms, Digital Criminology, Routine Activity Theory

I. INTRODUCTION AND BACKGROUND TO THE STUDY

The emergence and rapid diffusion of social media platforms across the Nigerian digital ecosystem have fundamentally reconfigured the nature of social interaction, information dissemination, and community formation among the country's youth population. With approximately 137.8 million active internet users as of 2025, Nigeria possesses one of Africa's largest and most dynamically growing digital markets (BusinessDay, 2025). Within this expanding digital landscape, platforms such as X (formerly Twitter), Facebook, Instagram, and WhatsApp have become deeply embedded in the daily routines of young Nigerians, serving simultaneously as sites of social connection, economic opportunity, political mobilisation, and, increasingly, as arenas where criminal behaviour takes root and flourishes.

The relationship between social media and youth criminality in Nigeria has attracted growing scholarly attention over the past decade, though significant gaps remain in our understanding of the precise mechanisms through which digital platforms facilitate offending behaviour. Early research in this domain tended to focus narrowly on cybercrime as a discrete phenomenon, examining how young people engage in internet fraud, phishing, and identity theft (Tade, 2019). More recent scholarship, however, has begun to recognise that social media's influence extends considerably beyond these direct forms of digital offending. As Okafor, Enwezor, Anachuna, Etele, Mokwe, and Chukwu (2025) demonstrate in their study of secondary school students in Enugu State, social media exposure correlates not only with cybercrime involvement but also with broader patterns of behavioural change that may predispose young people towards various forms of criminal activity.

What makes this relationship particularly complex is the deeply ambivalent nature of social media itself. Monday, Adenuga, and colleagues (2025) characterize technology as a "digital double-edged sword" in their examination of Nigerian youth, highlighting how the same platforms that enable educational advancement, digital entrepreneurship, and civic participation simultaneously expose users to cybercriminal networks, fraudulent schemes, and harmful content. This duality presents considerable challenges for policymakers, educators, and parents seeking to maximize the benefits of digital engagement while minimizing its attendant risks. The question is not whether young Nigerians should use social media, such a proposition is both impractical and undesirable, but rather how they can be equipped to navigate these spaces safely and how platforms can be held accountable for the harms they facilitate.

Recent empirical evidence suggests the scale of these challenges is substantial. According to the Nigerian Communications Commission's 2025 Child Online Safety Report, an extraordinary 97% of Nigerian children have experienced some form of sexual exploitation while using the internet, with 89% reporting receipt of unsolicited sexual content or requests (AllAfrica, 2025). These figures, while alarming, represent only one dimension of a broader pattern of online harms affecting young Nigerians. Gatefield's State of Online Harms 2025 report estimates that 68.9 million Nigerians—fully half of the country's internet users, regularly encounter cyberbullying, online impersonation, scams, hate speech, and other forms of digital abuse (BusinessDay, 2025). Women and youth are disproportionately affected, with 58% of documented online harms targeting female users, particularly those in politics, media, or leadership positions.

The present study seeks to advance scholarly understanding of these phenomena through a comprehensive secondary analysis of existing research, survey data, and institutional reports. Rather than generating new primary data, the article synthesizes findings from multiple sources to construct a more integrated picture of how social media shapes youth criminal involvement across Nigeria's diverse regional and social contexts. This approach offers several advantages. It enables the

incorporation of data from studies conducted in different locations, from Ubasinachi's (2025) investigation of cybercrime in Nnewi commercial city to Ushie and Ndoma's (2024) research in Calabar Metropolis, allowing for identification of both common patterns and context-specific variations. It also facilitates the integration of quantitative prevalence data with qualitative insights into the lived experiences of young Nigerians navigating potentially harmful digital environments.

Several interrelated research questions guide this inquiry. First, what is the nature and extent of the relationship between social media usage patterns and youth involvement in criminal activities across Nigerian contexts? Second, through what specific mechanisms do social media platforms facilitate or amplify criminal behaviour among young users? Third, how adequate are existing legal frameworks and intervention strategies in addressing these challenges? Fourth, what theoretical frameworks best explain the observed relationships between digital engagement and offending behaviour? And finally, what evidence-based recommendations can be offered for policy, practice, and future research?

Addressing these questions requires careful attention to conceptual and definitional matters. The term "youth" is used throughout this article in accordance with the National Youth Policy's definition, encompassing individuals aged 18 to 35 years. "Criminal activities" is understood broadly to include both cyber-dependent crimes (those that can only be committed using digital technologies) and cyber-enabled crimes (traditional offences that may be amplified or facilitated by social media). This expansive definition reflects the reality that social media's criminogenic influence extends beyond obvious forms of digital fraud to encompass recruitment into offline criminal networks, exposure to extremist content, normalization of violence, and participation in various forms of online harassment and exploitation.

The article proceeds as follows. The next section reviews relevant literature, situating the current study within ongoing scholarly conversations about technology and crime in the Nigerian context. Section three outlines the theoretical framework, integrating

insights from Routine Activity Theory and Social Learning Theory. Section four describes the methodology employed in this secondary analysis. Section five presents findings organized thematically around key research questions. Section six discusses the implications of these findings for theory, policy, and practice. The final section offers concluding reflections and directions for future research.

II. LITERATURE REVIEW

2.1 The Evolution of Social Media Usage Among Nigerian Youth

Understanding the relationship between social media and youth criminality requires first appreciating how deeply these platforms have become embedded in the everyday lives of young Nigerians. The past decade has witnessed remarkable growth in both internet penetration and social media adoption across the country. According to data from the Nigerian Communications Commission, active internet subscriptions grew from approximately 92 million in 2019 to over 157 million by mid-2025, representing a penetration rate of roughly 70% of the population (NCC, 2025). Within this expanding digital ecosystem, youth constitute the most active and engaged segment, spending an average of four to six hours daily on various social media platforms.

This pattern of intensive engagement reflects broader transformations in Nigerian youth culture. As Monday, Adenuga, and colleagues (2025) observe, social media has become "deeply intertwined with identity formation, relationship maintenance, and status negotiation among young Nigerians." Platforms like Instagram and TikTok serve not merely as communication tools but as arenas for performing identity, displaying consumption, and establishing social standing. WhatsApp groups function as virtual communities where peer norms are reinforced and collective identities are forged. X (formerly Twitter) operates as a site of political discourse, cultural critique, and, increasingly, as a battleground where reputation is contested and sometimes destroyed.

The COVID-19 pandemic accelerated these trends considerably. With schools closed and physical movement restricted during 2020 and 2021, young

Nigerians turned to social media for education, entertainment, and social connection in unprecedented numbers (Oyedemi & Mogano, 2021). This period of intensified engagement may have had lasting effects on usage patterns, normalizing levels of screen time that would previously have been considered excessive. It may also have exposed a new cohort of young users to online risks at developmentally vulnerable stages, with consequences that are only now becoming apparent in the research literature.

2.2 Cybercrime and Youth Offending in Nigerian Scholarship

Nigerian criminological research has devoted considerable attention to youth involvement in cybercrime, particularly the phenomenon popularly known as "Yahoo Yahoo" or, in its more technologically sophisticated variant, "Yahoo Plus." Early studies in this tradition tended to focus on individual-level factors associated with cybercrime involvement, including socioeconomic deprivation, peer influence, and moral disengagement (Tade, 2013; Aransiola & Asindemade, 2011). This body of work established that many young Nigerians turn to cyber fraud not primarily because of psychological pathology but rather in response to structural conditions of unemployment, limited opportunity, and perceived relative deprivation.

More recent scholarship has adopted a more nuanced perspective, recognizing that cybercrime among Nigerian youth cannot be understood in isolation from broader patterns of social media usage and digital culture. Okafor et al. (2025) examined the relationship between social media exposure and cybercrime involvement among senior secondary school students in Udi Local Government Area of Enugu State. Their findings revealed that students who spent more than three hours daily on social media platforms were significantly more likely to report engagement in, or knowledge of, cybercriminal activities. The study identified peer influence within social media networks as a particularly powerful predictor, suggesting that these platforms function as sites where deviant behaviour is normalized and even celebrated.

Ubasinachi (2025) explored similar themes in the context of Nnewi commercial city in Anambra State,

focusing specifically on what motivates youth engagement in cybercrime through social media. The research found that economic pressure, peer influence, and the perceived invisibility of online offending all contributed to involvement in cybercriminal activities. Notably, the study also examined the effectiveness of existing prevention strategies, concluding that disciplinary punishments alone are insufficient and must be complemented by educational interventions and technological solutions. The recommendation that "social media users must be careful when following links provided by unknown sources" reflects a broader emphasis on individual responsibility that characterizes much of this literature.

Ushie and Ndoma (2024) approached the issue from a different angle, examining the relationship between social media literacy and vulnerability to cybercrime in Calabar Metropolis, Cross River State. Their findings suggested that limited understanding of social media platforms' functioning, privacy settings, and risk indicators significantly increases the likelihood of falling victim to cybercrime. Importantly, the study also explored the potential of social media as a tool for crime prevention, finding that law enforcement agencies could more effectively deploy these platforms to monitor criminal activity and communicate safety information to the public. This dual focus, on both the risks and potential benefits of social media, represents an important advance in the literature.

2.3 Online Harms Beyond Cybercrime

While cybercrime has dominated scholarly attention, recent research has begun to document a broader range of online harms affecting Nigerian youth. The State of Online Harms 2025 report, produced by Gatefield in collaboration with Paradigm Initiative and Luminare, provides perhaps the most comprehensive picture to date (BusinessDay, 2025). Drawing on survey data from across Nigeria's six geopolitical zones, the report estimates that 50% of internet users experience online harms regularly, with the most common forms including misinformation and disinformation (identified as the primary digital threat), hate speech and incitement, cyberbullying and trolling, online impersonation and scams, gender-based harassment, and exposure to unsolicited pornography.

The distribution of these harms across platforms is uneven and instructive. X (formerly Twitter) accounts for 34% of reported online harms, the highest proportion among all platforms studied. This finding may reflect the platform's role as a site of political discourse, where partisan conflict and personal attacks frequently intersect. Facebook follows closely behind, characterized by the report as "overwhelmed by a significant scale of harmful content." WhatsApp, despite its encrypted nature, functions as a breeding ground for disinformation, with false narratives spreading rapidly through forwarded messages in group chats. These platform-specific patterns suggest that effective intervention strategies must be tailored to the distinctive affordances and user cultures of different social media environments.

The gender dimensions of online harm deserve attention. The Gatefield report found that 58% of online harms target women, especially those in politics, media, or leadership positions. This finding aligns with international research documenting the use of online abuse as a mechanism for policing women's participation in public life and reinforces calls for gender-sensitive approaches to digital safety. For young women, the consequences of online harassment extend beyond immediate psychological distress to include self-censorship, withdrawal from digital spaces, and diminished educational and professional opportunities.

2.4 Legal and Policy Responses

Nigeria has not been entirely passive in responding to the challenges posed by cybercrime and online harms. The Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 provides a legislative framework for addressing various forms of digital offending, including identity theft, child pornography, cyberstalking, and computer-related fraud. The Act establishes offences, prescribes penalties, and creates institutional mechanisms for enforcement, including the office of the National Cybercrime Coordinator. More recently, President Bola Tinubu's administration has indicated its intention to review and strengthen existing legislation, including the Child Rights Act (2003) and the Violence Against Persons (Prohibition) Act (2015), to better address online forms of abuse (AllAfrica, 2025).

However, the adequacy of these legal frameworks remains a subject of considerable debate. Critics argue that the Cybercrime Act, while well-intentioned, has been unevenly enforced and may in some instances be used to suppress legitimate expression rather than target genuine criminal activity (Ewang, 2025). The absence of explicit provisions addressing platform accountability means that social media companies operating in Nigeria face limited legal pressure to moderate harmful content effectively or to cooperate with law enforcement in investigating offences. As Ewang (2025) argues in her advocacy for stronger regulation, "platforms built to connect us are failing to protect our most vulnerable," and legislative action is urgently needed to mandate robust content moderation, establish local accountability mechanisms, and impose meaningful penalties for non-compliance.

The Child Online Access Protection Bill, currently under consideration by the National Assembly, represents a potential step forward. Sponsored by Olumide Osoba, Chairman of the House Committee on Justice, the proposed legislation seeks to mandate internet service providers to restrict access to violent or exploitative content, penalize individuals and organizations engaged in cyberbullying or the dissemination of intimate images of minors, promote digital literacy education, and establish mechanisms for prompt reporting and redress of online abuse (BusinessDay, 2025). Whether the bill will pass in its current form and, if enacted, prove effective in achieving its objectives, remains to be seen.

2.5 Gaps in the Literature

Despite the valuable contributions of existing research, significant gaps remain in scholarly understanding of social media's relationship to youth criminality in Nigeria. First, most studies have focused on cybercrime to the exclusion of other forms of online harm, leaving the connections between social media engagement and offline criminal behaviour relatively underexplored. Second, the literature has tended to treat youth as an undifferentiated category, obscuring important variations by age, gender, socioeconomic status, and geographical location. Third, longitudinal research capable of tracking changes in social media usage and criminal involvement over time is almost

entirely absent, limiting the ability to draw causal inferences about the direction of relationships. Fourth, theoretical development has lagged empirical investigation, with many studies adopting implicit or ad hoc explanatory frameworks rather than engaging systematically with established criminological theory. The present study seeks to address some of these gaps through comprehensive secondary analysis and theoretical integration.

III. THEORETICAL FRAMEWORK

Understanding the relationship between social media and youth criminality requires theoretical tools capable of explaining how digital environments shape behaviour, facilitate offending, and condition the responses of potential victims and guardians. This article draws on two complementary theoretical traditions within criminology: Routine Activity Theory and Social Learning Theory. Each offers distinctive insights into the mechanisms linking social media engagement to criminal involvement, and together they provide a more comprehensive explanatory framework than either could achieve alone.

3.1 Routine Activity Theory

Originally formulated by Cohen and Felson (1979) to explain patterns of predatory crime in physical space, Routine Activity Theory has proven remarkably adaptable to the analysis of digital offending. The theory's core proposition is elegantly simple: for a crime to occur, three elements must converge in time and space, a motivated offender, a suitable target, and the absence of capable guardianship. Crime rates fluctuate not primarily because of changes in offender motivation but because of shifts in the routine activities that bring these elements together.

Applying this framework to social media and youth criminality illuminates several important dynamics. First, social media platforms substantially expand the pool of potential targets accessible to motivated offenders. Whereas traditional offending required physical proximity to victims, digital platforms enable young people in Nigerian cities to target individuals anywhere in the world, dramatically increasing the opportunities for fraud, extortion, and exploitation.

The suitability of these targets is enhanced by the wealth of personal information users voluntarily share online, which offenders can exploit to craft convincing phishing attempts or manipulate victims through social engineering.

Second, social media transforms the nature of guardianship in ways that may increase offending opportunities. Capable guardianship in digital spaces might take various forms: platform content moderation, parental supervision, peer intervention, or law enforcement monitoring. Yet evidence suggests these guardianship mechanisms are frequently absent or ineffective. As Ewang (2025) notes, 60% of Nigerians who report harmful content see no action taken on their complaints, and 31% of reported content is never removed from platforms. The absence of meaningful consequences for offending may lower the perceived risks associated with criminal behaviour, encouraging further engagement.

Third, the routine activities of young Nigerians increasingly involve substantial time spent on social media platforms, creating concentrated periods of exposure to potential offending opportunities. When large numbers of motivated young people, many experiencing economic pressure and limited legitimate opportunities, congregate in digital spaces where suitable targets abound and capable guardians are absent, Routine Activity Theory would predict elevated rates of criminal behaviour. The theory thus directs attention not to individual pathology but to the structural conditions that bring offenders, targets, and the absence of guardianship together in social media environments.

3.2 Social Learning Theory

While Routine Activity Theory explains the convergence of conditions necessary for crime, Social Learning Theory, as developed by Akers (1998), illuminates the processes through which individuals acquire criminal definitions and learn offending techniques. Drawing on Sutherland's differential association theory and incorporating insights from behavioural psychology, Social Learning Theory proposes that criminal behaviour is learned through interaction with others in a process involving four key

mechanisms: differential association, definitions, differential reinforcement, and imitation.

Social media platforms function as extraordinarily powerful sites for social learning about crime. Through differential association in digital spaces, young Nigerians encounter peers who may model criminal behaviour, express favourable definitions of offending, and reinforce deviant conduct through approval and admiration. The celebrity status sometimes accorded to successful fraudsters in popular culture, the "Yahoo boys" whose conspicuous consumption is displayed on Instagram, exemplifies how social media can communicate definitions favourable to crime. When young people observe peers acquiring wealth and status through offending, and when these observations are accompanied by narratives that neutralize moral concerns or portray victims as deserving, the likelihood of imitation increases substantially.

The technical dimensions of criminal learning are also facilitated by social media. Platforms host communities where offenders share techniques, exchange tools, and mentor newcomers in the skills required for successful offending. Phishing scripts, hacking tutorials, and guides to social engineering circulate through WhatsApp groups and Telegram channels, often protected from law enforcement scrutiny by encryption and ephemeral messaging features. This peer-to-peer transmission of criminal knowledge represents a form of learning that traditional criminological theories, developed in an era of face-to-face interaction, could not fully anticipate.

3.3 Integrating the Two Perspectives

Routine Activity Theory and Social Learning Theory, while distinct in their emphases, can be productively integrated to explain the relationship between social media and youth criminality. Routine Activity Theory explains why social media environments generate abundant offending opportunities, while Social Learning Theory explains how young people come to recognize and act upon these opportunities. The former addresses the structural conditions of digital spaces; the latter addresses the cultural and interactional processes through which criminal definitions are acquired and sustained.

This integrated framework suggests that interventions to reduce social media-facilitated criminality must operate at multiple levels. At the structural level, modifying routine activities might involve enhancing digital guardianship through improved platform moderation, strengthening legal accountability, and providing legitimate alternatives that reduce the time young people spend in high-risk online environments. At the cultural level, interventions might seek to counter definitions favourable to crime by promoting digital literacy, ethical reflection, and positive peer norms. Neither approach alone is likely to prove sufficient; both are required to address the complex dynamics through which social media shapes criminal involvement.

IV. METHODOLOGY

4.1 Research Design

This study employed a mixed-methods secondary analysis design, synthesizing quantitative and qualitative data from existing sources to examine the relationship between social media and youth criminality in Nigeria. Secondary analysis offers advantages for researching this topic, enabling the integration of findings from multiple studies conducted across different locations and time periods while avoiding the ethical and practical challenges of directly surveying vulnerable populations about sensitive topics (Heaton, 2004). The approach is consistent with recent calls in criminological research for greater use of existing data to address questions that cannot be adequately examined through primary data collection alone.

4.2 Data Sources

Data were drawn from four categories of sources. First, national survey data were obtained from the Nigerian Communications Commission's 2025 Child Online Safety Report and Gatefield's State of Online Harms 2025 report. These sources provide representative prevalence estimates and detailed information about the nature and distribution of online harms affecting Nigerian youth. Second, peer-reviewed journal articles published between 2020 and 2025 were systematically identified through searches of academic databases including African Journals

Online (AJOL), Google Scholar, and Scopus. Search terms included combinations of "social media," "youth," "cybercrime," "Nigeria," "online harms," and related variants. Studies were included if they reported empirical findings relevant to the research questions, employed clearly described methods, and focused on Nigerian populations.

Third, institutional reports and policy documents were obtained from government agencies, non-governmental organizations, and international bodies. These sources provided information about legal frameworks, intervention programmes, and institutional responses to online harms. Fourth, media reports from reputable Nigerian news organizations were consulted for contextual information and illustrative case material, though these were used primarily to supplement rather than substitute for scholarly sources.

4.3 Inclusion Criteria and Search Strategy

The search strategy prioritized recent publications to ensure findings reflected current patterns of social media usage and criminal involvement. Studies published before 2020 were included only if they addressed topics for which more recent research was unavailable or if they provided essential theoretical or historical context. Geographic coverage encompassed all regions of Nigeria, though the distribution of available research is uneven, with southern states more heavily represented than northern states. This geographic imbalance reflects broader patterns in Nigerian social science research and represents a limitation that future studies should address.

4.4 Data Extraction and Synthesis

From each included source, information was extracted regarding study characteristics (location, sample, design), key findings, and implications for understanding social media's relationship to youth criminality. Quantitative data were compiled in summary tables to facilitate comparison across studies and identification of common patterns. Qualitative findings were analyzed thematically, with attention to recurring themes, divergent perspectives, and contextual nuances that quantitative analysis might obscure. The synthesis process was iterative, moving

between examination of individual sources and development of broader interpretive frameworks.

4.5 Ethical Considerations

Secondary analysis of published data raises fewer ethical concerns than primary research with human participants, but several considerations nonetheless warrant attention. All sources used in this study were publicly available, and no individual-level identifying information was accessed or analyzed. Where studies reported sensitive information about criminal involvement, findings have been presented in aggregated form to protect participant confidentiality. The research was conducted in accordance with the University of Lagos ethical guidelines for studies involving secondary data.

4.6 Limitations

Several limitations of this approach should be acknowledged. Secondary analysis is constrained by the quality and coverage of available data, and gaps in the existing literature cannot be remedied through reanalysis. The geographic unevenness of research coverage means findings may not be equally applicable across all Nigerian regions. Variations in study designs, measurement approaches, and sampling strategies complicate direct comparison of findings across sources. Causality cannot be definitively established from cross-sectional data, and the direction of relationships between social media usage and criminal involvement remains uncertain. These limitations are addressed in the discussion section, where findings are interpreted with appropriate caution.

V. FINDINGS

5.1 Prevalence and Patterns of Online Harms

The secondary analysis reveals consistently high rates of online harms affecting Nigerian youth across multiple studies and data sources.

The consistency across these studies is striking despite their different methodologies, geographic foci, and target populations. The NCC finding that 97% of Nigerian children have experienced online sexual

exploitation demands attention, though the figure should be interpreted with recognition that "experience" encompasses a range of exposures from relatively minor to severely abusive. The Gatefield estimate that half of all Nigerian internet users regularly encounter online harms suggests these phenomena are not confined to vulnerable minorities but rather constitute widespread features of the digital environment.

5.2 Platform-Specific Patterns

The distribution of online harms across different social media platforms is uneven and instructive.

X's position as the platform accounting for the largest share of reported harms likely reflects its role as a site of political discourse and public argumentation. The platform's affordances, public by default, retweet functionality enabling rapid spread of content, minimal moderation relative to scale, create conditions conducive to conflict and abuse. Facebook's substantial share of harms reflects its massive user base and the platform's well-documented struggles with content moderation at scale. WhatsApp's role in disinformation dissemination highlights the challenges posed by encrypted platforms, where harmful content spreads through private networks inaccessible to external monitoring.

5.3 Mechanisms Linking Social Media to Criminal Involvement

The analysis identified several mechanisms through which social media facilitates youth involvement in criminal activities. These mechanisms operate at individual, interpersonal, and structural levels and interact in complex ways that simple explanatory models cannot capture.

Normalization of Deviant Behaviour: Across multiple studies, peer influence within social media networks emerged as a powerful predictor of criminal involvement. Okafor et al. (2025) found that students whose social media networks included peers engaged in cybercrime were significantly more likely to report favourable attitudes towards offending and, in some cases, participation in criminal activities themselves. This pattern aligns with Social Learning Theory's

emphasis on differential association as a mechanism for acquiring definitions favourable to crime. When young people observe peers achieving material success through offending, and when these observations are accompanied by narratives that neutralize moral concerns, the likelihood of imitation increases.

Technical Knowledge Transmission: Social media platforms function as sites for the dissemination of criminal techniques. Ubasinachi (2025) documented how phishing scripts, hacking tutorials, and guides to social engineering circulate through WhatsApp groups and Telegram channels. This peer-to-peer transmission of criminal knowledge lowers the technical barriers to entry for would-be offenders, enabling young people with limited computing skills to participate in sophisticated forms of cybercrime. The encryption and ephemeral messaging features that protect legitimate privacy concerns simultaneously shield these criminal learning networks from law enforcement scrutiny.

Exposure to Criminal Networks: For some young Nigerians, social media provides initial contact with organized criminal networks. Recruitment messages, whether direct or veiled, circulate through platforms, offering economic opportunities that may, on closer examination, prove to be criminal in nature. The economic pressures documented by Ubasinachi (2025) as primary motivators for cybercrime create a pool of vulnerable youth susceptible to such recruitment approaches.

Amplification of Victimization Risk: Social media usage increases exposure to potential victimization in ways that may, paradoxically, increase offending among some youth. Young people who fall victim to online scams or harassment may, in response, adopt protective behaviours that include learning about criminal techniques or, in some cases, transitioning from victim to offender. This victim-offender overlap, well documented in traditional criminological research, may be amplified in digital environments where the boundaries between victimization and offending are particularly fluid.

5.4 Demographic Variations

The available evidence suggests that the relationship between social media and criminal involvement varies across demographic categories. Gender differences are particularly pronounced. The Gatefield report's finding that 58% of online harms target women aligns with international research documenting the gendered nature of digital abuse (BusinessDay, 2025). However, the relationship between victimization and offending may differ by gender, with young men more likely to transition from social media engagement to active criminal participation, particularly in forms of cyber fraud.

Age differences also emerge from the analysis. The NCC's focus on children (defined as individuals under 18) reflects recognition that younger users face distinctive risks, including sexual exploitation and grooming (AllAfrica, 2025). Older youth, particularly those in the 18-25 age range, appear more likely to engage in instrumental offending such as fraud and scams, reflecting the economic pressures that intensify as young people transition to adulthood. These developmental differences have implications for intervention design, suggesting the need for age-appropriate approaches that address the distinctive vulnerabilities and motivations characterizing different life stages.

Geographic variations are suggested by the available data, though the uneven distribution of research limits confident conclusions. Studies conducted in southern states (Enugu, Anambra, Cross River, Ebonyi) dominate the literature, with northern Nigeria substantially underrepresented. Whether this geographic imbalance reflects genuine differences in the prevalence of social media-facilitated criminality or merely differential research attention cannot be determined from existing evidence.

5.5 Adequacy of Existing Responses

The analysis reveals widespread agreement among researchers and advocates that existing legal and institutional responses to online harms are inadequate. Ubasinachi (2025) found that while disciplinary punishments for cybercrime exist, they are insufficient to deter offending without complementary educational

and technological interventions. Ewang (2025) argues that platform accountability mechanisms are virtually absent, with 60% of user complaints producing no action and 31% of reported harmful content remaining online. The Child Online Access Protection Bill, while promising, remains under legislative consideration, and even if enacted will require robust implementation and enforcement to achieve its objectives.

Several studies emphasize the potential of digital literacy as a preventive strategy. Ushie and Ndoma (2024) found that limited understanding of social media platforms' functioning significantly increases vulnerability to cybercrime, suggesting that educational interventions could reduce harm by equipping young users with knowledge about privacy settings, risk indicators, and safe practices. Monday, Adenuga, and colleagues (2025) similarly call for "digital literacy curricula and cyber security awareness programs" as essential components of a comprehensive response to technology-related harms.

VI. DISCUSSION

6.1 Interpreting the Findings

The findings presented above paint a complex picture of the relationship between social media and youth criminality in Nigeria. On one hand, the prevalence estimates from national surveys are deeply concerning, suggesting that millions of young Nigerians regularly encounter online harms ranging from relatively minor annoyances to severe forms of exploitation and abuse. The 97% figure from the NCC report demands urgent policy attention and raises fundamental questions about the safety of digital spaces that have become central to youth social life.

On the other hand, careful interpretation of these figures is necessary to avoid alarmist conclusions that might justify overly restrictive responses. The NCC's finding that 97% of Nigerian children have "experienced" online sexual exploitation encompasses a wide range of exposures, from unsolicited sexual images to direct grooming and abuse. While all such experiences are harmful and warrant prevention efforts, the conflation of different severity levels in a single statistic can obscure important distinctions. Similarly, the Gatefield finding that 50% of internet

users experience online harms regularly includes diverse phenomena whose implications for youth development and well-being vary considerably.

The integration of Routine Activity Theory and Social Learning Theory offers a useful framework for making sense of these complexities. From a Routine Activity perspective, the high prevalence of online harms reflects structural features of digital environments that bring motivated offenders, suitable targets, and the absence of capable guardianship together on an unprecedented scale. The concentration of harms on specific platforms, X's disproportionate share, Facebook's scale challenges, WhatsApp's encryption dilemmas, reflects platform-specific variations in how these structural conditions manifest. Interventions informed by this perspective would target the environmental conditions that enable offending rather than focusing exclusively on individual offenders or victims.

Social Learning Theory illuminates the cultural and interactional processes through which young people come to define certain forms of online behaviour as acceptable or desirable. The normalization of cybercrime within some peer networks, the transmission of criminal techniques through WhatsApp groups, and the celebrity status accorded to successful fraudsters on Instagram all exemplify learning processes that encourage rather than discourage offending. Interventions informed by this perspective would seek to counter definitions favourable to crime by promoting alternative norms, values, and role models within the same digital spaces where criminal learning currently occurs.

6.2 Implications for Policy and Practice

The findings carry several implications for policy and practice. First, there is a clear need for enhanced legal frameworks that explicitly address platform accountability. The Cybercrime Act of 2015, while an important first step, does not adequately address the responsibility of social media companies to moderate harmful content, cooperate with law enforcement, and protect vulnerable users. The Child Online Access Protection Bill, if enacted and properly implemented, could fill some of these gaps, though its ultimate

effectiveness will depend on enforcement mechanisms and resources.

Second, digital literacy education should be prioritized at all levels of the educational system. Ushie and Ndoma's (2024) finding that limited understanding of social media increases vulnerability to cybercrime suggests that equipping young people with knowledge about platform functioning, privacy settings, and risk indicators could meaningfully reduce harm. Such education should begin early, before children encounter significant online risks, and should be reinforced throughout secondary and tertiary education. It should also extend beyond technical knowledge to include ethical reflection on the consequences of online behaviour for oneself and others.

Third, economic interventions that address the structural conditions driving some youth toward cybercrime are essential. Ubasinachi's (2025) finding that economic pressure is a primary motivator for cybercrime involvement underscores the limitations of purely legal or educational responses. Young people facing limited legitimate opportunities for economic advancement will remain vulnerable to recruitment into criminal networks regardless of their digital literacy or knowledge of legal consequences. Job creation, skills training, and entrepreneurship support should therefore be understood as components of a comprehensive strategy for reducing online offending.

Fourth, platform-specific interventions tailored to the distinctive affordances and user cultures of different social media environments are needed. The concentration of harms on X suggests the need for enhanced moderation of political discourse and more effective responses to harassment. WhatsApp's role in disinformation dissemination calls for user education about verifying forwarded content and, potentially, platform-level changes that slow the spread of viral misinformation. Facebook's scale challenges require continued investment in content moderation capacity and algorithmic detection of harmful content.

6.3 Theoretical Implications

The findings also carry implications for criminological theory. The application of Routine Activity Theory to

digital environments reveals both the theory's continued relevance and its need for adaptation. The concepts of motivated offenders, suitable targets, and capable guardianship translate reasonably well to online spaces, but the mechanisms through which they converge differ from physical environments in important ways. Temporal and spatial convergence, central to the original formulation, operates differently when offenders and targets may never share physical space and when guardianship is exercised by algorithms and content moderators rather than by people physically present. These differences suggest the need for continued theoretical refinement.

Social Learning Theory similarly requires adaptation to digital contexts. The mechanisms of differential association, definitions, differential reinforcement, and imitation all operate online, but they do so through affordances, likes, shares, comments, algorithmic amplification, that the theory's originators could not have anticipated. The speed and scale of learning in digital environments, where criminal techniques can be transmitted to thousands of potential offenders simultaneously, challenges assumptions about learning as an incremental process occurring within small groups. These observations point toward the need for a digital criminology that retains the insights of established theories while adapting them to the distinctive features of online environments.

6.4 Limitations and Future Research Directions

Several limitations of this study should inform interpretation of its findings and guide future research. The secondary analysis approach, while valuable for synthesizing existing evidence, cannot overcome gaps or weaknesses in the underlying literature. The geographic unevenness of research coverage, with southern states overrepresented and northern states underrepresented, limits confidence in the generalizability of findings across Nigeria's diverse regions. Future research should prioritize data collection in understudied areas, including the northern states where cultural, economic, and technological conditions may differ substantially from the contexts examined in existing studies.

Longitudinal research capable of tracking changes in social media usage and criminal involvement over

time is urgently needed. The cross-sectional design of most existing studies precludes confident conclusions about causal direction, leaving open the possibility that pre-existing tendencies toward offending shape social media usage patterns rather than the reverse. Longitudinal studies following cohorts of young people from early adolescence through young adulthood could clarify these temporal dynamics and identify critical periods for intervention.

Research examining the effectiveness of existing interventions is also needed. While many studies recommend digital literacy programmes, enhanced legal frameworks, and economic interventions, evidence on what works in the Nigerian context remains limited. Rigorous evaluation research, including randomized controlled trials where feasible, could generate the evidence base needed to guide policy and practice decisions.

Finally, research should attend more carefully to the positive dimensions of social media engagement. The focus on harms and criminality in this study, while justified by the research questions, should not obscure the substantial benefits that social media provides to Nigerian youth. Understanding how young people use these platforms for education, entrepreneurship, civic engagement, and social connection is essential for developing balanced approaches that maximize benefits while minimizing risks.

VII. CONCLUSION

This article has examined the relationship between social media and youth involvement in criminal activities in Nigeria through a comprehensive secondary analysis of existing research, survey data, and institutional reports. The findings reveal that online harms affect a substantial proportion of Nigerian youth, with prevalence estimates ranging from 50% of all internet users experiencing regular harms to 97% of children encountering some form of online sexual exploitation. These figures, while alarming, require careful interpretation that distinguishes among different types of harm and attends to the contexts in which they occur.

The analysis identified multiple mechanisms linking social media to criminal involvement, including the

normalization of deviant behaviour through peer networks, transmission of technical knowledge for offending, exposure to criminal recruitment, and amplification of victimization risk. These mechanisms operate within platform-specific environments that shape the nature and distribution of harms. X accounts for the largest share of reported harms, followed by Facebook and WhatsApp, each presenting distinctive challenges for prevention and intervention.

The integrated theoretical framework combining Routine Activity Theory and Social Learning Theory proved valuable for making sense of these complexities. Routine Activity Theory illuminates the structural conditions, convergence of motivated offenders, suitable targets, and absent guardianship, that make social media environments conducive to crime. Social Learning Theory explains the cultural and interactional processes through which young people acquire definitions favourable to offending and learn criminal techniques from peers. Together, these perspectives suggest that effective responses must operate at multiple levels, addressing both environmental conditions and cultural norms.

The policy implications of this research are clear. Nigeria requires enhanced legal frameworks that mandate platform accountability, robust enforcement mechanisms, and meaningful penalties for non-compliance. Digital literacy education should be prioritized at all educational levels, equipping young people with the knowledge and skills to navigate online spaces safely. Economic interventions addressing the structural conditions that drive some youth toward offending are essential components of a comprehensive strategy. Platform-specific approaches tailored to the distinctive features of different social media environments are needed.

Yet legislation and programmes alone cannot solve these challenges. The deeper issue concerns the values and norms that shape online behaviour and the economic structures that condition youth responses to limited legitimate opportunity. Addressing social media-facilitated criminality ultimately requires building a society where young people have meaningful alternatives to offending, where digital spaces are designed with safety as a priority rather than an afterthought, and where the dignity and rights of all

users are respected. These are ambitious goals, but the evidence reviewed in this article suggests that failing to pursue them will carry substantial costs for Nigerian youth and for Nigerian society as a whole.

REFERENCES

- [1] Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Northeastern University Press.
- [2] AllAfrica. (2025, October 27). Nigeria: 9 in 10 Nigerian children face online risks – Report. *AllAfrica*. <https://allafrica.com/stories/202510280043.html>
- [3] Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759-763. <https://doi.org/10.1089/cyber.2010.0307>
- [4] BusinessDay. (2025, October 26). 68.9m of Nigeria's internet users experience cyberbullying, scams, child sexual abuse – Report. *BusinessDay*. <https://businessday.ng/news/article/68-9m-of-nigerias-internet-users-experience-cyberbullying-scams-child-sexual-abuse-report/>
- [5] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608. <https://doi.org/10.2307/2094589>
- [6] Ewang, S. (2025, December 2). Nigeria's children are unsafe online. The law must step up. *TheCable*. <https://www.thecable.ng/nigerias-children-are-unsafe-online-the-law-must-step-up/>
- [7] Heaton, J. (2004). *Reworking qualitative data*. Sage Publications.
- [8] Monday, O., Adenuga, G., & [others]. (2025). Technology and the Nigerian youth: An examination of the impact of the digital double-edged sword. *Pakistan Journal of Integrated Social Sciences*, 2(2). <https://doi.org/10.51846/pjiss.v2i2.4600>
- [9] Nigerian Communications Commission. (2025). *Child Online Safety Report 2025*. NCC Publications.
- [10] Okafor, J. N., Enwezor, H. C., Anachuna, O. N., Etele, V. A., Mokwe, N. F., & Chukwu, P. O. (2025). Impact of social media on senior secondary school students' involvement in cybercrime in Udi Local Government Area of Enugu State, Nigeria. *European Scientific Journal*, 21(16), 107-128. <https://doi.org/10.19044/esj.2025.v21n16p107>
- [11] Oyedemi, T., & Mogano, S. (2021). The digitally dispossessed: Digital divide and youth in South Africa and Nigeria during the COVID-19 pandemic. *Information Development*, 37(4), 567-580. <https://doi.org/10.1177/02666669211019456>
- [12] Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'Yahoo Plus' phenomenon. *Human Affairs*, 23*(4), 689-705. <https://doi.org/10.2478/s13374-013-0158-3>
- [13] Tade, O. (2019). Recruitment into cybercrime among Nigerian youth. In S. Hales & S. R. Stoneman (Eds.), *The Oxford handbook of cyberpsychology*. Oxford University Press.
- [14] Ubasinachi, R. O. (2025). Influence of social media on cybercrime prevalence among the youth of Nnewi commercial city [Unpublished undergraduate project]. Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State.
- [15] Ushie, C. U., & Ndoma, R. N. (2024). Social media literacy and cybercrime: A study of Calabar Metropolis, Cross River, Nigeria. *Lwati: A Journal of Contemporary Research*, 21(1), 87-104. <https://www.ajol.info/index.php/lwati/article/view/268178>