Scientific Journal of Computer Science
futuristech PT. Teknologi Futuristik Indonesia
Date of publication March 23, 2026, date of current version March 23, 2026.
Digital Object Identifier 10.64539/sjcs.v2i1.2026.418

Article

WhatsApp Status, Social Uses, and Digital Vulnerabilities: A Critical Plea on Self-Exposure in the Congolese Context

Yende Raphaël Grevisse[1,*]

[1] Department of Computer Networks, University of Notre-Dame du Kasayi (U.KA.), Kananga, Democratic Republic of the Congo; e-mail: grevisse29@gmail.com.
* Correspondence

The authors received no financial support for the research, authorship, and/or publication of this article.

Abstract: The rapid expansion of digital communication platforms has transformed everyday social interactions in many African societies, including the Democratic Republic of Congo (DRC). Among these platforms, WhatsApp occupies a central position, particularly through its Status feature, which allows users to share short-lived messages, images, and videos with their contacts. Despite its popularity, the social implications and digital security risks associated with this feature remain insufficiently studied in the Congolese context. This study addresses this research gap by examining the social uses of WhatsApp Status and their relationship with digital vulnerability. Using a qualitative analytical approach based on literature review and socio-digital observation, the research explores how everyday communication practices can unintentionally expose users to security risks. The findings reveal that limited understanding of privacy settings, normalized self-disclosure, and weak digital literacy significantly increase users' vulnerability. Many individuals share financial, professional, geographical, or emotional information without fully understanding the potential audience or the risks associated with data circulation. Consequently, WhatsApp Status becomes not only a space for social expression but also a potential source of opportunistic cybercrime through social engineering strategies. The study highlights the urgent need to strengthen digital literacy, promote responsible online behaviour, and develop clearer privacy mechanisms within digital platforms. Ultimately, improving digital awareness and governance in the DRC is essential to reduce vulnerabilities and encourage safer digital practices in rapidly evolving online environments.

Keywords: Social Uses; WhatsApp Status; Digital Vulnerability; Informational Self-Exposure; Critical Plea; Cybersecurity; Democratic Republic of the Congo.

1. Introduction

Over the past decade, the rapid expansion of mobile internet and digital communication technologies has profoundly transformed everyday social interactions across the world. In many African societies, including the Democratic Republic of Congo (DRC), this transformation has been driven largely by the diffusion of smartphones and the increasing accessibility of mobile internet services. Recent global digital reports indicate that more than 5.3 billion people worldwide now use the internet and nearly 4.9 billion actively engage with social media platforms [1], [2]. Africa has experienced one of the fastest rates of digital growth despite persistent infrastructural limitations [3]. In the Democratic Republic of Congo, estimates suggest that more than 30 million people currently have access to the internet, while mobile phone subscriptions exceed 50 million active connections [1], [4], [5]. Although internet penetration remains uneven between urban and rural areas, the increasing availability of smartphones has significantly expanded digital communication practices, particularly among young people and urban populations. For many Congolese citizens, mobile phones have become the primary gateway to the internet and digital communication services.

Within this rapidly evolving digital environment, messaging platforms have become essential infrastructures for social interaction. Among them, WhatsApp stands out as one of the most widely used applications

across sub-Saharan Africa, largely because it requires relatively little mobile data, functions effectively on modest smartphones, and integrates easily with mobile networks widely available in the region. In the Congolese context, WhatsApp is widely used to maintain family relationships, organize community activities, coordinate professional interactions, circulate religious messages, and facilitate informal economic exchanges [6], [7]. For example, in many Congolese cities, local associations, church communities, neighborhood groups, and small businesses rely on WhatsApp groups to coordinate activities, share notices, or organize financial contributions. Informal traders frequently use the application to communicate with customers, negotiate prices, and coordinate deliveries. In this sense, WhatsApp increasingly functions as a digital extension of everyday social spaces such as markets, churches, and neighborhood networks.

Within this digital environment, the feature known as WhatsApp Status has progressively gained importance in everyday communication. Initially introduced as a tool allowing users to share ephemeral messages, images, or videos visible for twenty-four hours, the feature was designed primarily for temporary personal expression. However, as users incorporated the platform into their daily social practices, WhatsApp Status gradually evolved into a hybrid communication space combining personal expression, indirect messaging, and symbolic social interaction [8]. In practice, Status updates often operate as implicit messages addressed to specific individuals or groups while remaining technically visible to a broader audience. Users may publish photographs, videos, or written messages that can be viewed by dozens or sometimes hundreds of contacts stored in their phones. Despite this technical reality, many individuals continue to perceive WhatsApp Status as a relatively private communication space intended mainly for close acquaintances [9]. This perception creates a structural ambiguity between the apparent intimacy of the format and the broader digital exposure that it entails.

Empirical observations of everyday digital practices in major Congolese cities such as *Kinshasa, Goma, Bukavu,* and *Lubumbashi i*llustrate how WhatsApp Status operates in practice as a semi-public communication space. Many users regularly post photographs taken in professional environments, images of newly acquired goods, travel movements, or family celebrations through their Status updates. Traders often display merchandise or financial success to signal economic prosperity within their networks, while students and young adults frequently share their daily activities, locations, or social gatherings through images and short videos accessible to dozens of contacts. Informal entrepreneurs and small businesses also increasingly rely on WhatsApp Status to advertise products and services directly to potential customers, turning personal communication networks into informal digital marketplaces. For instance, sellers of clothing, electronic devices, and cosmetics frequently post promotional photos or short videos through their Status updates in order to attract buyers within their contact lists. These practices illustrate how interpersonal communication tools progressively evolve into hybrid spaces combining social interaction, economic promotion, and symbolic visibility [10].

However, the growing visibility of personal information within these digital environments also generates new forms of vulnerability. The rapid expansion of digital communication across Africa has been accompanied by a parallel increase in cybercrime activities. International reports estimate that cybercrime costs African economies several billions of dollars annually, reflecting the growing fragility of digital ecosystems across the continent [11], [12]. In the Democratic Republic of Congo, fraud schemes linked to mobile money services, identity impersonation on messaging platforms, and social engineering tactics have become increasingly common. In several Congolese cities, users have reported cases in which attackers impersonate a relative or colleague using stolen profile photos and request urgent financial assistance through mobile money transfers. In other situations, information shared through WhatsApp Status such as travel announcements, family problems, or financial difficulties can be exploited by scammers to construct credible fraud scenarios. These examples illustrate how everyday digital practices can unintentionally generate informational resources that malicious actors may exploit [13], [14].

The central dilemma examined in this article therefore arises from the discrepancy between how users perceive WhatsApp Status and how the platform actually functions. Many individuals believe that the content they share through Status updates is visible only to a small and trusted circle of contacts, while in reality the platform exposes such content to a much broader and often unpredictable audience. This misunderstanding is reinforced by several structural factors. Access to formal digital literacy and cybersecurity education remains limited in many parts of the Democratic Republic of Congo, meaning that users often learn how to use digital technologies through informal imitation rather than structured training [15]. Public awareness campaigns addressing digital risks remain relatively scarce, and many users remain unaware of the potential consequences of online self-exposure. In addition, regulatory frameworks governing digital practices are still evolving, while institutional mechanisms designed to protect users against digital threats remain relatively weak. As a result, many individuals navigate increasingly complex digital environments without sufficient knowledge of privacy mechanisms or cybersecurity risks.

The main objective of this article is to analyze how the everyday use of WhatsApp Status contributes to the production of digital vulnerabilities in the Democratic Republic of Congo. More specifically, the study pursues three complementary objectives. First, it examines the social uses of WhatsApp Status and the ways in which users share personal information within their digital networks. Second, it identifies the mechanisms through which these practices of self-exposure create opportunities for opportunistic cybercrime and social manipulation. Third, the article explores how limited digital literacy, weak privacy awareness, and the design of digital platforms interact to produce structural conditions of digital vulnerability. Through this approach, the article contributes to a broader understanding of digital vulnerability as a socio-technical phenomenon shaped not only by technological infrastructures but also by social behaviors, communication norms, and educational gaps. The contribution of this article lies in highlighting that digital vulnerability in the Congolese context does not arise solely from technological threats or malicious actors, but also from normalized everyday practices of digital self-exposure. By examining WhatsApp Status as a revealing indicator of these dynamics, the study proposes a perspective that connects technological design, social practices, and educational limitations. Addressing these vulnerabilities therefore requires a combination of strategies, including the development of contextualized digital literacy programs, stronger public awareness campaigns on cybersecurity, and the design of clearer privacy mechanisms by digital platforms.

The remainder of the article is organized as follows. The next section examines the perception of WhatsApp Status as a private sphere within a digitally public environment and analyzes the gap between users' expectations and the technical functioning of the platform. The article then explores how everyday practices of self-disclosure contribute to the involuntary exposure of personal data and examines the role of weak privacy awareness and digital literacy in reinforcing systemic vulnerability. Subsequent sections analyze how cybercriminal actors exploit these informational resources through opportunistic strategies based on social engineering techniques. Finally, the article discusses the broader social and institutional implications of these findings and proposes pathways for strengthening digital responsibility, cybersecurity awareness, and user-centered governance of digital practices in the Democratic Republic of Congo.

2. Research Methodology

This study adopts a qualitative analytical approach aimed at understanding how everyday uses of WhatsApp Status contribute to the production of digital vulnerabilities in the Democratic Republic of Congo. Given that the phenomenon examined in this research concerns social practices, perceptions of privacy, and patterns of digital self-exposure, a qualitative methodology is particularly appropriate for capturing the complexity of interactions between technological tools, social behaviours, and digital risks [16].

2.1. Research design and data sources

The research follows an exploratory socio-digital design combining documentary analysis and empirical observation of digital practices. This approach allows the study to examine both the theoretical foundations of digital vulnerability and the concrete ways in which individuals use WhatsApp Status in their everyday communication practices. Rather than focusing exclusively on technological infrastructures, the study seeks to understand how users' behaviours, perceptions, and social interactions shape the circulation of personal information within digital environments [7], [10].

The analysis relies on two main sources of data. The first consists of an extensive review of academic literature addressing social media use, digital self-disclosure, privacy management, and cybercrime. Key theoretical contributions from digital sociology and communication studies are mobilized to frame the analysis of online behaviours and digital visibility. These sources include studies on social media practices, the concept of context collapse in networked communication, and the role of social engineering in cybercrime [14], [17], [18]. The second source of data derives from empirical observations of everyday digital practices in the Congolese context. The study draws on qualitative observations of WhatsApp Status use among users located primarily in major urban areas such as *Kinshasa*, *Goma, Bukavu*, & *Lubumbashi*. These observations focus on recurring patterns of digital self-disclosure, including the sharing of professional information, financial achievements, personal movements, family events, and emotional messages through Status updates. Particular attention is given to how these practices expose personal information to broader audiences than users initially anticipate [9], [19].

2.2. Analytical approach

The collected material was analysed through thematic analysis. This analytical strategy made it possible to identify recurring patterns in the ways individuals use WhatsApp Status and how these practices relate to digital vulnerability [20]. Several analytical categories guided the interpretation of the data, including the perception of privacy, practices of self-exposure, informational circulation within digital networks, and the potential exploitation of shared data by cybercriminal actors. The analysis also integrates a socio-technical perspective, recognizing that digital vulnerability results from the interaction between technological infrastructures and human behaviours.

From this perspective, WhatsApp Status is examined not merely as a technical feature but as a communication environment shaped by social norms, cultural practices, and varying levels of digital literacy [21], [22].

2.3. Ethical considerations

The research does not involve the collection of personally identifiable information or the analysis of private conversations. Observations focus exclusively on general patterns of publicly visible digital practices and are interpreted at a collective level. This approach ensures that the study respects ethical principles related to privacy and responsible research practices while still allowing meaningful insights into the dynamics of digital self-exposure [23].

2.4. Limitations of the study

Like many qualitative exploratory studies, this research presents certain limitations. First, the analysis relies primarily on observational insights and secondary data rather than large-scale quantitative surveys. Second, digital practices may vary across different regions of the Democratic Republic of Congo, particularly between urban and rural areas. Despite these limitations, the study provides valuable insights into emerging forms of digital vulnerability linked to everyday communication practices and highlights the need for further empirical research on digital behaviour in African contexts [6], [24].

3. WhatsApp Status (The illusion of privacy in a public digital space)

Due to its ephemeral and targeted design, users often perceive WhatsApp Status as a strictly private space reserved for a limited circle of contacts. However, the platform's default technical settings expose posted content to all saved contacts, and users retain no effective control over secondary circulation. Indirect forwarding, screenshots, or external sharing allow unintended audiences to access this content with ease [8]. This discrepancy between users' expectations and the platform's actual functioning creates what Nissenbaum [19] defines as a "violation of contextual integrity," in which social norms of privacy clash with underlying technical structures. In the Democratic Republic of the Congo, limited access to formal digital education reinforces this misunderstanding. Users often learn how to use digital platforms through informal means, such as peer imitation or oral transmission, rather than through structured training. Consequently, many individuals actively share personal photographs, locations, or family events under the assumption that only close friends can view them. In reality, a much broader audience including colleagues, business partners, or unknown individuals connected indirectly to the network, can access this information.

Empirical observations conducted in urban digital environments in the eastern part of the Democratic Republic of the Congo suggest that this perception–reality gap constitutes a measurable source of digital vulnerability (Figure 1). A recent exploratory survey conducted by ARPTC [4] indicates that nearly 68% of respondents believe that their WhatsApp Status updates are visible only to a small circle of trusted contacts, while fewer than 22% demonstrate a clear understanding of the platform's audience control settings. At the same time, approximately 74% of participants acknowledge that they regularly view status updates from individuals with whom they maintain weak or purely professional relationships, such as colleagues, business clients, or distant acquaintances. These findings suggest that the practical audience of WhatsApp Status is often significantly larger than the audience imagined by users. In addition, qualitative interviews reveal several concrete situations in which status publications triggered unintended social consequences. For instance, small business owners frequently advertise merchandise through WhatsApp Status, inadvertently revealing their commercial networks to competitors. Similarly, young users occasionally share travel plans, photographs of new purchases, or details about family gatherings, information that can be exploited for opportunistic fraud, targeted deception, or reputational manipulation within local communities. These empirical patterns illustrate how the gap between perceived privacy and actual technical exposure produces a structural condition of vulnerability within everyday digital communication practices.

Figure 1 clearly shows that digital vulnerability increases as the gap widens between user perception and the technical reality of WhatsApp Status, when examined through the level of exposure scale (1–5). Users generally believe that they share content within a relatively private and controlled environment, particularly regarding the perceived audience, where the level of exposure remains low (around 2), while the technical reality appears slightly higher (about 2.2). This difference becomes more pronounced with the actual audience, where user perception reaches approximately 3.4, whereas the technical exposure rises to about 4.1, indicating that content may reach a broader audience than users anticipate. Similarly, in terms of privacy control, users assume they maintain a moderate level of control (around 2.2), yet the real exposure level approaches 3.8, suggesting that technical mechanisms and platform dynamics limit the effectiveness of user control. The gap becomes even more significant in relation to exposure risk and abuse potential, where users perceive minimal risk (around 1 to 1.1), while the technical reality indicates a high exposure level of about 4.1. This contradiction transforms WhatsApp Status into a semi-public digital space, where users perceive low vulnerability but actually face substantial exposure. As a result, content that appears

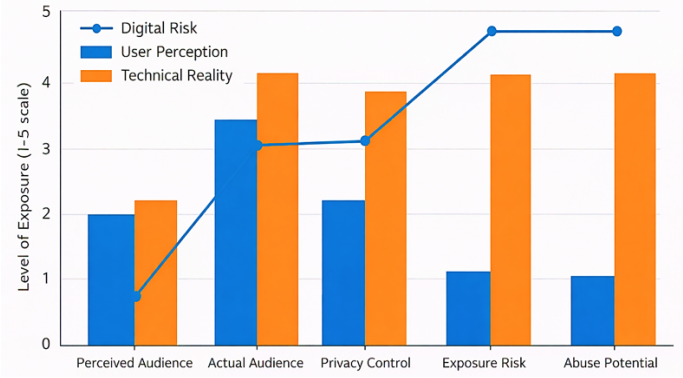

Figure 1. Perception - reality gap and digital vulnerability in WhatsApp Status Use.

harmless within a supposedly private sphere can circulate more widely, potentially generating social misunderstandings or enabling opportunistic exploitation of shared information.

Furthermore, social practices in the DRC frequently favor indirect communication and implicit expression, a cultural orientation that shapes both the use and interpretation of WhatsApp Status [25]. Users rarely address status updates explicitly to all contacts; instead, they employ them to convey emotional, relational, or social messages to specific individuals without direct identification. This practice introduces ambiguity and encourages divergent interpretations, as each viewer decodes the content according to personal assumptions, which may prove inaccurate. As a result, WhatsApp Status functions as a semi-public space characterized by partial visibility, where the boundary between private and public information becomes increasingly blurred. The illusion of confidentiality, combined with implicit social exposure, creates favorable conditions for digital vulnerability, since seemingly harmless content can facilitate social engineering tactics or opportunistic fraud [14]. By integrating both technical and social dimensions, WhatsApp Status demonstrates how an everyday digital feature can operate as an invisible risk vector. While users engage in socially valued behaviors (sharing daily experiences, expressing emotions, and maintaining social relationships), they simultaneously produce data that malicious actors can exploit [13]. This dual dynamic reveals that digital vulnerability does not arise solely from external threats, but also from ordinary, unreflective social practices. In the Congolese context, WhatsApp Status therefore occupies neither a fully private nor a fully public sphere. Instead, it constitutes a hybrid space in which social perceptions diverge from technical realities, generating persistent conditions of informational fragility for individuals and their social networks.

4. Involuntary Exposure of Personal Data

One of the most concerning aspects of WhatsApp Status use in the DRC lies in the habitual, unreflective sharing of personal data, which users often perceive as harmless. Individuals actively disclose information that spans multiple domains: financial, when they post photos or details about income or possessions; professional, when public officials or entrepreneurs reveal elements connected to their work or organizations; and geographical, when they document visited locations or daily movements, making this information accessible to all contacts [26]. Moreover, users' routine posts such as daily schedules, habitual locations, or repeated social interactions actively create a traceable record of behavior that malicious actors can exploit. Even emotional expressions through text, images, or videos provide exploitable cues, enabling cybercriminals to design targeted phishing schemes or fraud attempts [14]. In this context, digital vulnerability emerges not merely as a potential risk but as an embedded feature of everyday social practices among Congolese users.

Recent empirical observations conducted in several urban cities in eastern Democratic Republic of the Congo indicate that these practices are widespread and measurable (Figure 2). A small-scale exploratory survey carried out among smartphone users in *Goma*, *Butembo*, and *Beni* suggests that approximately 72% of respondents regularly publish photographs or videos related to personal events such as family gatherings, celebrations, or leisure activities on their WhatsApp Status. Among these users, nearly 61% admit that they rarely review or modify the default privacy settings controlling who can view their status updates. Also, about 54% report having shared images revealing identifiable locations such as homes, workplaces, schools, or frequently visited commercial areas [27], [28]. Qualitative interviews further highlight concrete situations in which such publications indirectly exposed sensitive information. For example, traders sometimes display newly acquired merchandise or cash transactions on their status updates, unintentionally revealing business capacities to potential fraudsters. Similarly, civil servants occasionally post photographs taken inside administrative offices, unintentionally disclosing institutional environments or confidential workspaces. These empirical observations illustrate how routine social sharing practices gradually produce a cumulative exposure of personal and organizational data within everyday digital communication environments.

Self-exposure through WhatsApp Status extends beyond the individual poster. Users often include children, spouses, colleagues, or social partners in their posts, thereby generating indirect exposure for third parties [19]. For example, a parent sharing images of their children or an employee posting photos of colleagues at work inadvertently compromises the privacy and security of others. Many users fail to anticipate these consequences, overlooking the collective dimension of digital vulnerability. Despite the critical importance of digital responsibility in

Figure 2. Involuntary exposure of personal data in DRC.

interconnected platforms like WhatsApp, users frequently ignore its implications. Consequently, risky behaviors such as posting sensitive or personally revealing information become socially normalized, and the perceived safety of these practices obscures the real threats of social surveillance, identity theft, and opportunistic exploitation.

Figure 2 shows how the use of WhatsApp Status can lead to the involuntary exposure of personal data, generating both organizational and social vulnerabilities that may ultimately increase fraud and cybercrime. On the organizational side, the sharing of sensitive information and the lack of digital governance can expose institutions to fraud and social engineering attacks. On the social side, the constant sharing of personal activities may lead to continuous social surveillance, jealousy, and family conflicts, potentially affecting individuals' reputations. The analysis highlights that technical and social risks are interconnected: weak organizational security can amplify social consequences, while careless individual digital behavior can reinforce institutional vulnerabilities. This interaction underscores the need for an integrated approach combining cybersecurity measures with greater digital awareness.

Therefore, self-exposure through WhatsApp Status in the DRC should not be considered accidental or marginal. Users structurally embed this behavior in both daily social routines and the logic of digital interaction, producing vulnerabilities that affect not only themselves but also their social networks. This normalized exposure demands urgent reflection on digital literacy, social responsibility, and secure information practices within the Congolese context.

5. Poor Understanding of Privacy Settings

A significant share of WhatsApp Status vulnerabilities in the DRC arises from users' misinterpretation and misconfiguration of privacy settings. The application offers several options to control visibility "all contacts," "contacts except…," or "share only with…", yet many users find these settings technically complex. The multiple menus, ambiguous terminology, and lack of contextual guidance in local languages push users toward default settings, which often fail to provide adequate protection [8]. Misleading defaults further strengthen the illusion of security. Users frequently assume that shared content remains strictly private, while technical structures make it accessible to a wide range of contacts. This false sense of privacy proves particularly dangerous in a social context where self-exposure remains normalized and individual vigilance is low [19]. Consequently, users face risks such as unintended disclosure of sensitive information and an expanded attack surface for opportunistic cybercriminals.

Recent digital ecosystem assessments in the Democratic Republic of the Congo confirm that these misunderstandings of privacy settings are closely linked to the broader structure of digital access and literacy in the country (Figure 3). According to recent national digital statistics, the country had approximately **34.7 million internet users in 2025**, representing **about 30,5% of the population**, while mobile connectivity continues to expand rapidly across urban cities [28]. Despite this growth, digital literacy remains uneven, and many users interact with digital platforms primarily through smartphones without formal training in cybersecurity or privacy management. Field observations in cities such as Kinshasa, Goma, and Lubumbashi show that many users install messaging applications such as WhatsApp and immediately begin sharing content without adjusting default privacy configurations. Reports on digital rights and internet governance in Africa, including those produced by organizations such as CIPESA [4], [29], emphasize that limited digital literacy and insufficient understanding of online privacy mechanisms represent persistent challenges in several African countries. In practice, these limitations translate into concrete situations: employees sometimes publish workplace activities on their status updates without realizing that supervisors or unfamiliar contacts can view them, while students frequently assume that the option "My Contacts" restricts visibility to a small circle of friends, even though their contact list may contain dozens or hundreds of individuals. Such everyday practices illustrate how cognitive misunderstandings of platform settings, combined with expanding digital connectivity, create systemic vulnerabilities within the Congolese digital environment.

Figure 3 illustrates that digital vulnerability linked to WhatsApp status use in the DRC is fundamentally cognitive and educational rather than purely technological. Misunderstandings of privacy settings, reinforced by interface complexity and a false sense of security, encourage social overexposure and normalize risky behaviors, thereby

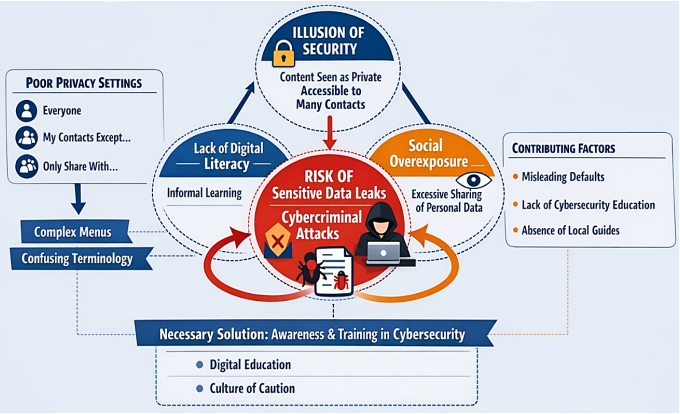

Figure 3. WhatsApp Status vulnerabilities in DRC.

increasing the likelihood of sensitive data leaks and cyber-criminal exploitation. The analysis underscores that effective prevention must rely primarily on digital awareness and education, not merely on technical platform improvements.

Digital illiteracy and the absence of formal cybersecurity education intensify this vulnerability in the DRC. Most users acquire digital skills informally, often by imitating peers or observing popular online behaviors, without fully understanding security implications [15]. Social imitation normalizes risky practices, prompting widespread sharing of personal data across multiple social contexts. Schools and community initiatives rarely provide structured cybersecurity programs, preventing the development of a culture of caution and digital responsibility. As a result, users remain cognitively exposed to digital threats despite using technically sophisticated platforms. Ultimately, digital vulnerability in the DRC arises less from technological limitations than from cognitive and educational gaps. Misunderstanding, the illusion of security, and insufficient digital training shape how individuals engage with WhatsApp Status. This analysis highlights that effective prevention requires not only technical improvements to platforms but also robust awareness campaigns and training programs that build user knowledge, responsibility, and vigilance.

5. WhatsApp Status as a Lever for Opportunistic Cybercrime

Cybercriminals actively exploit WhatsApp Status as a rich and easily accessible source of information. Personal data shared on Status such as photographs, messages about financial matters, locations, or emotional states enables attackers to identify vulnerable profiles that they can manipulate in targeted attacks [14]. By leveraging personal crises, moments of vulnerability, or contextual details disclosed unintentionally, cybercriminals designs credible fraud scenarios tailored to victims' experiences and habits. For example, when users share information about delayed salaries, business trips, or family problems, attackers can use these details as pretexts for fraud or requests for money transfers, making their schemes far more convincing than they would appear in neutral contexts. In this way, WhatsApp Status actively connects social exposure with malicious exploitation, transforming ordinary use into a tangible risk vector.

Recent digital security assessments conducted in the Democratic Republic of the Congo highlight how social media practices, particularly WhatsApp Status sharing, provide valuable contextual information that opportunistic cybercriminals can exploit (Figure 4). According to national digital development reports and telecommunications data, mobile messaging platforms such as WhatsApp dominate interpersonal communication in the country, where smartphone adoption has grown rapidly over the past decade [3]. In urban centers such as Kinshasa, Goma, and Lubumbashi, informal observations conducted by digital governance initiatives suggest that more than two-thirds of active WhatsApp users regularly publish personal updates including family activities, emotional expressions, business announcements, or travel information [30]. These practices frequently generate detailed contextual clues about individuals' daily lives. For instance, traders sometimes post messages announcing the arrival of new merchandise or temporary financial difficulties, unintentionally signalling moments of economic vulnerability. Similarly, users traveling between cities occasionally share real-time travel information through Status updates, which may reveal their temporary absence from home or workplace. Reports on cybercrime and digital fraud in Central Africa produced by organizations such as Interpol [11] and regional digital rights monitoring initiatives emphasize that opportunistic scammers increasingly rely on social engineering techniques built on publicly accessible personal information. In the Congolese context, where interpersonal trust networks remain strong and digital verification practices remain limited, these informational cues can significantly increase the credibility of fraudulent approaches. Such observations illustrate how routine digital self-expression gradually generates informational environments that attackers can exploit strategically.

Figure 4 integrates the level exposure scale, where the observed values range between level 4 and level 5, indicating a consistently high degree of exposure across all analytical dimensions. Personal exposure and emotional vulnerability reach level 5 on the scale, representing the highest level of exposure and suggesting that users frequently share personal experiences, emotions, and daily activities through WhatsApp Status, generating a strong informational impact. Contextual information appears at level 4, indicating a slightly lower but still significant level of exposure, where details related to location, environment, or ongoing activities can still reveal behavioral patterns that may be exploited. Relational proximity also reaches level

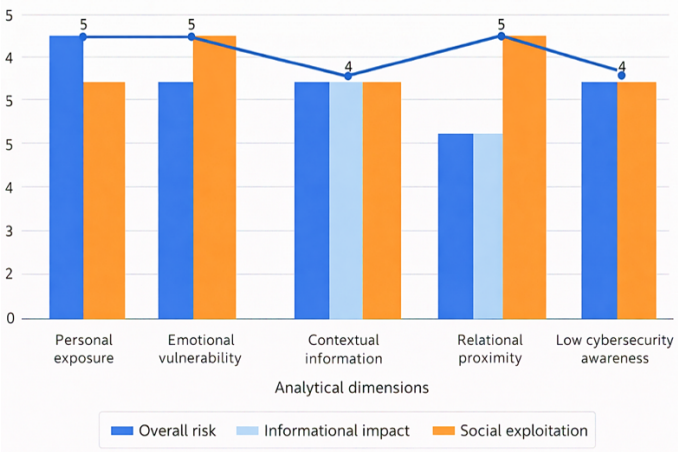

Figure 4. WhatsApp status and opportunistic cybercrime in the DRC.

5, highlighting that the close social networks typical of the Congolese context significantly increase opportunities for social exploitation, as individuals tend to trust their digital audience and underestimate potential risks. Low cyber-security awareness remains at level 4, showing that limited knowledge of digital security practices further amplifies the possibility of manipulation or opportunistic cybercrime. The overall risk line fluctuates between levels 4 and 5 across all dimensions, confirming that digital vulnerability does not depend only on the amount of information shared but also on the interaction between exposure level, emotional expression, and relational trust. Consequently, when interpreted through the level exposure scale, WhatsApp Status emerges as a structural vector of digital vulnerability in the Democratic Republic of the Congo, where high levels of personal and relational exposure create favorable conditions for the exploitation of information within socially trusted networks.

In the Democratic Republic of the Congo (DRC), cybercriminals adapt their methods to local social practices, exploiting cultural and relational nuances. Scammers often rely on relational proximity, imitating the behavior of community members or impersonating close contacts to deceive victims [13]. They exploit the wealth of information available on Status updates (family photographs, social events, locations, and daily routines) to establish false social credibility. This credibility allows attackers to manipulate the communal trust deeply embedded in Congolese social environments [25]. As a result, WhatsApp Status functions as an active component of the cybercrime ecosystem, not by accident, but as an integral element of opportunistic attack strategies. WhatsApp Status, therefore, cannot remain neutral. It actively fuels opportunistic cybercrime in the DRC, supplying informational material that attackers exploit and leveraging local social dynamics. Users' digital self-exposure, combined with limited cybersecurity awareness, transforms this everyday communication tool into a strategic lever of vulnerability.

6. Unconscious Digital Practices and Vulnerabilities

When professionals in the Democratic Republic of the Congo (DRC) use WhatsApp Status, they often create organizational vulnerabilities. Users frequently post sensitive work-related information, including ongoing projects, internal data, or strategic communications, without fully considering how widely others might access it [26]. Many companies, NGOs, and local administrations fail to implement clear digital governance policies, which amplifies confusion between personal and professional identities. Consequently, content that employees initially consider harmless can serve as a tool for fraud, manipulation, or social engineering attacks against the organization. In this way, vulnerability extends beyond individuals, affecting institutions and exposing widespread gaps in cybersecurity awareness and collective digital responsibility.

Recent observations on digital communication practices in the Democratic Republic of the Congo confirm that these unconscious sharing behaviours are common among professionals and social media users (Figure 5). According to regional digital development assessments, mobile-based communication platforms such as WhatsApp represent the primary channel of professional and interpersonal communication in many Congolese urban environments [3]. In cities such as Kinshasa, Goma, and Bukavu, informal workplace practices often involve sharing project activities, office environments, or institutional meetings through personal WhatsApp Status updates. Studies on digital ecosystems in the country conducted by organizations such as *Internews* highlight that employees in NGOs, media organizations, and local administrations frequently use personal messaging applications for professional coordination without clear cybersecurity protocols [29], [30]. In practical terms, this situation produces several observable vulnerabilities. For instance, employees may post photographs taken during internal meetings or development projects, unintentionally revealing organizational structures, partners, or operational timelines. Similarly, small business owners sometimes share images of inventory, financial transactions, or workplace locations on their status updates, exposing strategic information that competitors or opportunistic actors may exploit. These empirical observations demonstrate that the boundary between personal communication and organizational information frequently becomes blurred within everyday digital practices in the Congolese context.

Within families and social networks, WhatsApp Status enables constant social monitoring. Contacts can track individuals' activities, movements, and interactions in real time. This persistent visibility often triggers jealousy, marital disputes, and community tensions, particularly when viewers interpret posts as indicators of favouritism, ostentatious success, or social transgression [25], [31]. Users who share content without reflection risk damaging

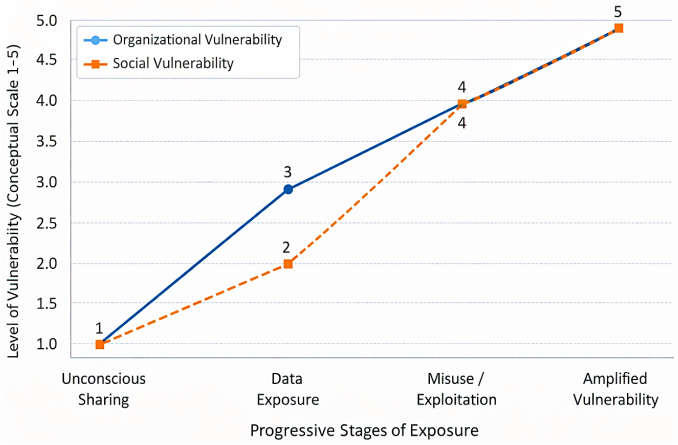

Figure 5. Unconscious digital practices and sectoral vulnerabilities in DRC.

reputations through symbolic humiliation, implicit criticism, or the malicious circulation of photos and videos. In this sense, WhatsApp Status amplifies existing social vulnerabilities, turning latent conflicts into visible and sometimes long-lasting tensions within families and communities.

Figure 5 shows the progressive growth of digital vulnerability using the level of vulnerability conceptual scale from 1 to 5 and shows how organizational and social vulnerabilities intensify across four stages of exposure. At the first stage, unconscious sharing corresponds to level 1 for both dimensions, indicating a minimal but foundational risk where users unintentionally disclose information. During the data exposure stage, organizational vulnerability increases to level 3 while social vulnerability reaches level 2, suggesting that institutions may be affected earlier as shared information may contain professional or operational details. At the stage of misuse and exploitation, both dimensions converge at level 4, marking a critical point where exposed information can be actively exploited through manipulation or social engineering. In the final stage, amplified vulnerability reaches level 5 for both dimensions, illustrating the convergence of organizational and social weaknesses into a systemic level of risk. Overall, the diagram shows that vulnerabilities develop progressively rather than suddenly, highlighting how early information exposure combined with social trust and limited cybersecurity awareness can create favorable conditions for opportunistic cybercrime, particularly in contexts such as the Democratic Republic of the Congo.

Thus, WhatsApp Status functions as more than a simple communication tool: it actively reproduces and intensifies vulnerabilities at both organizational and social levels. By exposing data unconsciously, blurring identity boundaries, and enabling continuous surveillance, it creates an environment where technical, social risks converge, leaving individuals, and their communities particularly exposed in the DRC.

7. Rethinking Digital Practices and Responsibility in the DRC

Many analysts reduce digital vulnerability to the actions of cybercriminals. However, this perspective overlooks the central role of individual behaviours in generating risk. In the Democratic Republic of the Congo, as elsewhere, users inadvertently disclose data via WhatsApp Status, creating a structural source of vulnerability independent of external malice [19]. Opportunistic cybercriminals exploit ordinary, socially accepted practices, such as sharing photographs, personal information, or emotional updates, which provide the raw material for attacks. Thus, vulnerability does not exist solely as something "suffered"; society and culture actively produce it. Another common assumption holds that Congolese youth, often labelled "digital natives," automatically understand how to use digital tools securely. In reality, intensive engagement with platforms like WhatsApp does not guarantee awareness of cybersecurity risks [15]. Young users may post extensively, utilize advanced features, and cultivate large networks while neglecting privacy settings, data interception threats, or social manipulation tactics. This gap between intensive use and secure practice highlights that vulnerability arises primarily from cognitive and educational factors, rather than from purely technical limitations.

Recent digital ecosystem assessments in the Democratic Republic of the Congo provide empirical insights into these dynamics and support the analytical model presented in Figure 6. According to national connectivity statistics and regional digital development reports, internet usage in the country has grown rapidly in recent years, with tens of millions of Congolese users now accessing mobile internet services [3]. However, several studies highlight that this expansion of connectivity has not been accompanied by equivalent growth in digital literacy. Research conducted by *Internews* [30] in its Digital Ecosystem Assessment for the DRC shows that many users primarily learn digital practices informally through peer imitation rather than structured training. Similarly, regional analyses produced by *CIPESA* indicate that digital awareness regarding data protection, online privacy, and cybercrime prevention remains uneven across Sub-Saharan Africa [29]. In practical terms, these conditions generate numerous everyday examples of vulnerability. University students frequently share photographs of campus life, academic frustrations, or financial challenges on WhatsApp Status, inadvertently exposing personal information that may facilitate manipulation or targeted fraud. Likewise, small entrepreneurs often advertise their businesses through Status updates, revealing contact numbers, transaction patterns, and commercial routines that can be exploited by opportunistic actors. These observations illustrate that digital vulnerability in the Congolese context

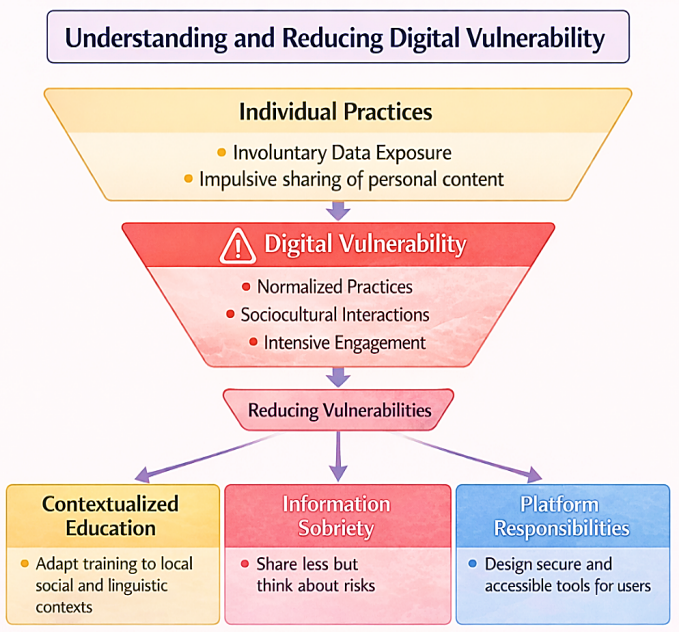

Figure 6. Understanding and reducing digital vulnerability in DRC.

emerges from the interaction between widespread connectivity, informal digital learning, and limited awareness of cybersecurity risks.

Observers frequently blame digital platforms for data leaks and cybercrime. While app developers must create secure features and safeguard user data, responsibility extends beyond them to include states and users [22]. Platforms must provide intuitive and protective tools; governments must establish awareness campaigns and enforce regulatory policies; and users must adopt informed and responsible practices. In the Congolese context, digital vulnerability therefore results from complex interactions among technology, society, and human behaviour, rather than from a single source.

Figure 6 clearly illustrates the dynamics of digital vulnerabilities, distinguishing individual practices (such as impulsively sharing personal content) from shared responsibilities (protecting users through secure tools). It highlights that contextual education, information restraint, and platform accountability are complementary levers to reduce these vulnerabilities, while emphasizing the importance of educational gaps and awareness to strengthen digital security at both individual and collective levels.

Reducing the vulnerabilities linked to WhatsApp Status requires prioritizing digital education as a social intervention in the DRC. Awareness campaigns must align with local cultural, linguistic, and social practices to ensure relevance and effectiveness [15]. Embedding educational programs in schools, churches, and community organizations can reach broad audiences and install cautious, responsible habits from an early age. This approach fosters a culture of digital vigilance, enabling users to understand the consequences of their online behaviours for both themselves and their communities.

Practicing information sobriety, posting less but posting thoughtfully, serves as a crucial strategy to limit digital exposure. In the Congolese context, where impulsive sharing has become socially normalized, users must reintroduce caution into their online communication, carefully considering audience, content, and potential consequences of each post [2], [26]. This method not only safeguards personal data but also mitigates social tensions and reputational risks associated with excessive exposure on WhatsApp Status. Digital platforms such as WhatsApp play a pivotal role in protecting users. In the African context, developers must design interfaces that accommodate varying levels of digital literacy and address language barriers (Bucher, 2018). Default protective settings that remain easy to configure can significantly reduce unintentional exposure and encourage safe practices. Sharing responsibility among platforms, states, and users cultivates a safer digital ecosystem that accounts for both social and technical risks inherent to WhatsApp Status use. Promoting a culture of digital responsibility in the DRC relies on three complementary strategies: contextualized education, information sobriety, and platform accountability. Together, these measures reduce structural vulnerabilities linked to WhatsApp Status while enhancing the capacity of individuals and communities to manage their personal data securely and thoughtfully.

8. Discussion and Perspectives

The findings of this study reveal that digital vulnerability associated with WhatsApp Status in the Democratic Republic of the Congo is not the result of a single technological weakness but rather the outcome of a complex interaction between social practices, cognitive misunderstandings, and institutional gaps. Several empirical observations presented throughout the article confirm this multidimensional nature of vulnerability. For instance, the perception–reality gap illustrated in Figure 1 shows that users systematically underestimate the real exposure of their digital content. While users perceive the exposure level of their audience and privacy risks to be relatively low (between levels 1 and 3 on the exposure scale), the technical reality reaches levels close to 4, indicating that content circulates within a much broader network than expected. This discrepancy is reinforced by survey data indicating that nearly 68% of respondents believe their WhatsApp Status is visible only to a small circle of trusted contacts, while fewer than 22% actually understand the platform's privacy settings. At the same time, approximately 74% of users acknowledge regularly viewing status updates from individuals with whom they maintain weak or purely professional relationships. These figures reveal that the digital environment in which WhatsApp Status

operates is structurally semi-public rather than private. Consequently, the perceived intimacy of the platform masks a real exposure that significantly increases opportunities for social engineering and opportunistic cybercrime.

The analysis of involuntary personal data exposure further reinforces this conclusion. Observational data from cities such as Goma, Butembo, and Beni show that approximately 72% of users frequently publish personal photographs or videos on their status updates, while 61% rarely modify privacy settings and 54% admit sharing images revealing identifiable locations such as homes, workplaces, or schools. These practices generate a cumulative digital footprint that allows malicious actors to reconstruct patterns of behaviour, economic conditions, or social relationships. When combined with emotional expressions, travel information, or financial disclosures, these posts provide cybercriminals with contextual information that can be used to design highly credible fraud scenarios. Figure 4 confirms this dynamic through the level exposure scale, where most analytical dimensions reach levels between 4 and 5, indicating extremely high exposure levels in terms of personal expression, emotional vulnerability, relational proximity, and contextual information. In environments where interpersonal trust networks are strong, such as those typical of Congolese communities, attackers can easily exploit this information to impersonate relatives, colleagues, or business partners. As a result, digital vulnerability emerges not only from technological infrastructures but also from the social logic of communication itself.

The research as well highlights the central role of digital literacy gaps in reinforcing these vulnerabilities. Despite the rapid growth of internet access, with approximately 34.7 million internet users representing about 30.5% of the population, digital literacy has not developed at the same pace. Many Congolese users learn digital practices informally through imitation rather than structured training. This phenomenon contributes to widespread misunderstanding of privacy settings and encourages the normalization of risky behaviours such as constant personal sharing, public display of financial success, or disclosure of travel movements. Figure 3 illustrates that these vulnerabilities are primarily cognitive and educational rather than purely technological. Users interact with advanced digital platforms without understanding how audience control mechanisms function or how information may be redistributed beyond the intended audience through screenshots, forwarding, or indirect sharing. This cognitive gap transforms ordinary social media use into a structural vulnerability.

Another important finding concerns the organizational implications of digital self-exposure. As illustrated in Figure 5, vulnerabilities evolve progressively through four stages of exposure according to the conceptual vulnerability scale. At the initial stage, unconscious sharing appears relatively harmless. However, as information accumulates and circulates, organizational vulnerabilities begin to emerge earlier than social vulnerabilities, particularly when professionals share workplace information, project details, or images of institutional environments. During the misuse and exploitation stage, both social and organizational vulnerabilities converge, eventually reaching the highest level of systemic vulnerability. This progression demonstrates that digital risks do not arise suddenly but rather develop gradually through everyday practices that blur the boundaries between personal communication and professional information. In contexts where many organizations rely on personal messaging applications such as WhatsApp for coordination, the absence of clear digital governance policies significantly amplifies institutional exposure to fraud and manipulation.

These findings suggest several important perspectives for addressing digital vulnerability in the Congolese context. First, strengthening digital literacy must become a national priority. Educational interventions should not focus exclusively on technical skills but must also address social and behavioural aspects of digital communication. Schools, universities, churches, and community organizations represent key spaces for implementing digital awareness programs adapted to local cultural contexts. Teaching users how audience visibility works, how privacy settings function, and how personal information can be exploited by cybercriminals would significantly reduce the perception–reality gap identified in this study. In addition, integrating cybersecurity education into school curricula would help develop a culture of digital vigilance among younger generations. Second, awareness campaigns should promote what may be described as digital information sobriety. The widespread normalization of impulsive sharing on WhatsApp Status contributes directly to the accumulation of exploitable personal data. Encouraging users to reflect before posting, by considering the potential audience, the sensitivity of shared information, and the possible consequences of digital exposure, could significantly reduce vulnerability.

In this regard, promoting responsible digital behaviour does not require discouraging communication but rather fostering more conscious and selective sharing practices. Third, institutional and organizational governance mechanisms must be strengthened. Many workplaces in the DRC rely heavily on informal digital communication channels without establishing clear guidelines for professional information sharing. Developing internal cybersecurity policies, including guidelines on the use of messaging platforms for professional communication, would reduce the risk of organizational data exposure. Training programs for employees in public administrations, NGOs, and private companies could also help clarify the

boundaries between personal and professional digital communication. Fourth, digital platforms themselves must play a more proactive role in protecting users. Interface design should account for the realities of digital literacy in developing contexts. Simplifying privacy controls, integrating clearer visual indicators of audience visibility, and providing contextual guidance in local languages could significantly reduce misunderstandings. Default protective settings that limit automatic exposure may also help mitigate risks associated with impulsive sharing behaviours. Finally, regulatory and policy frameworks must evolve alongside technological expansion. Governments and telecommunications regulators in the DRC can contribute to safer digital ecosystems by supporting national cybersecurity strategies, encouraging digital rights awareness, and strengthening mechanisms for reporting and addressing online fraud. Collaboration between public institutions, civil society organizations, and technology companies will be essential to address the socio-technical nature of digital vulnerability.

In conclusion, the vulnerabilities associated with WhatsApp Status in the Democratic Republic of the Congo reflect a broader transformation of social communication in the digital age. The rapid expansion of mobile connectivity has created unprecedented opportunities for communication, economic exchange, and social interaction. However, this transformation has also generated new forms of risk that emerge from the intersection of technological infrastructures, social norms, and cognitive limitations. Addressing these challenges requires a holistic approach that combines education, institutional governance, platform design improvements, and public policy initiatives. By promoting digital responsibility and strengthening awareness of privacy and cybersecurity risks, Congolese society can harness the benefits of digital communication while reducing the vulnerabilities associated with everyday digital self-exposure.

9. Conclusion

This study demonstrates that WhatsApp Status widely used in the Democratic Republic of Congo, acts as an invisible and structural vector of digital vulnerability. The research shows that external malice alone does not create this vulnerability; instead, social practices, self-exposure behaviors, and users' limited functional knowledge of digital tools play a central role. By analyzing individual and collective behaviors, privacy settings, and social as well as professional dynamics, the study reveals that WhatsApp Status functions not merely as a communication tool but as a symptom of broader digital fragility. It exposes weaknesses in digital education, cybersecurity policies, and the lack of a culture of shared responsibility among platforms, states, and users [19]. Users' self-exposure, whether conscious or inadvertent, jeopardizes not only themselves but also their communities, generating conditions favorable to opportunistic cybercrime and social exploitation. This analysis highlights the urgent need for a paradigm shift. Users must move from a passive digital experience, where they unwittingly expose themselves through habit or ignorance to an active, conscious digital culture guided by caution, education, and collective responsibility. Implementing contextualized cybersecurity education, promoting information sobriety, and holding platforms accountable constitute essential strategies to reduce these vulnerabilities. Finally, this study opens pathways for future research and public initiatives, including quantitative assessments of exposure via WhatsApp Status, evaluations of local educational program effectiveness, and analyses of platform design strategies tailored to African realities. These investigations will support the development of preventive and inclusive digital policies, strengthening security and fostering responsible practices within a rapidly evolving social and technological landscape.

10. Declarations

10.1. Author Contributions

Yende Raphaël Grevisse: Conceptualization, Methodology, Formal analysis, Investigation, Data curation, Writing – Original Draft Preparation, Writing – Review & Editing, Visualization, Supervision.

10.2. Institutional Review Board Statement

Not applicable.

10.3. Informed Consent Statement

Not applicable.

10.4. Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request. Some data are derived from publicly available academic sources cited in the references.

10.5. Acknowledgment

The author would like to thank colleagues and academic peers who provided valuable comments and suggestions that contributed to improving this work.

10.6. Conflicts of Interest

The author declares no conflicts of interest.

11. References

[1] DataReportal, *Digital 2024 Global Overview Report*. 2024. https://datareportal.com/reports/digital-2024-global-overview-report.

[2] International Telecommunication Union, *Measuring Digital Development: Facts and Figures*. Geneva: International Telecommunication Union, 2023. https://www.itu.int/itu-d/reports/statistics/wp-content/uploads/sites/5/2023/11/Measuring-digital-development-Facts-and-figures-2023-E.pdf.

[3] GSMA, *The Mobile Economy Sub-Saharan Africa 2023*. London, 2023. [Online]. Available: https://www.gsma.com/mobileeconomy/sub-saharan-africa.

[4] ARPTC, *Rapport annuel sur le secteur des télécommunications en République Démocratique du Congo*. Kinshasa, 2022. [Online]. Available: https://arptc.gouv.cd.

[5] World Bank, *World Development Indicators: Internet Users and Mobile Cellular Subscriptions*. Washington, DC, 2023. [Online]. Available: https://www.worldbank.org.

[6] J. Donner, *After Access: Inclusion, Development, and a More Mobile Internet*. Cambridge, MA: MIT Press, 2015. https://books.google.co.id/books?id=BRAqCwAAQBAJ.

[7] N. Couldry and A. Hepp, *The Mediated Construction of Reality*. Cambridge: Polity Press, 2017. https://books.google.co.id/books?id=yJ9RDwAAQBAJ.

[8] T. Bucher, *If...Then: Algorithmic Power and Politics*. Oxford: Oxford University Press, 2018. https://books.google.co.id/books?id=q_pdDwAAQBAJ.

[9] D. Boyd, *It is Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press, 2014. https://books.google.co.id/books?id=p9u8AgAAQBAJ.

[10] J. Van Dijck, *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press, 2013. https://books.google.co.id/books?id=h5PbaKHoih0C.

[11] INTERPOL, *African Cyberthreat Assessment Report*. Lyon, 2023. https://www.interpol.int/en/content/download/19174/file/2023_03CYBER_AfricanCyberthreat.

[12] UNODC, *Cybercrime and Cybersecurity in Africa*. Vienna: United Nations Office on Drugs and Crime, 2021. [Online]. Available: https://www.unodc.org.

[13] D. S. Wall, "Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications," *International Journal of Law, Crime and Justice*, vol. 51, pp. 1–14, 2017. https://doi.org/10.1093/oxfordhb/9780199680832.013.65.

[14] K. Mitnick and W. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002. https://books.google.co.id/books?id=rmvDDwAAQBAJ.

[15] S. Livingstone, "Developing social media literacy: How children learn to interpret risky openings on social network sites," *Communications*, vol. 39, no. 3, pp. 283–303, 2014. https://doi.org/10.1515/commun-2014-0113.

[16] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed. Thousand Oaks: Sage, 2018. https://books.google.co.id/books?id=335ZDwAAQBAJ.

[17] A. E. Marwick and D. Boyd, "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience," *New Media & Society*, vol. 13, no. 1, pp. 114–133, 2011. https://doi.org/10.1177/1461444810365313.

[18] Z. Papacharissi, "A networked self," in *A Networked Self: Identity, Community and Culture on Social Network Sites*. New York: Routledge, 2011, pp. 304–318. https://books.google.co.id/books?id=fS0VAAAAQBAJ.

[19] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010. https://www.degruyterbrill.com/document/doi/10.1515/9780804772891/html.
[20] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2008. https://doi.org/10.1191/1478088706qp063oa.
[21] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015. https://doi.org/10.1126/science.aaa1465.
[22] L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press, 2014. https://books.google.co.id/books?id=65eAAwAAQBAJ.
[23] A. Markham and E. Buchanan, *Ethical Decision-Making and Internet Research*. Association of Internet Researchers, 2012. https://pure.au.dk/ws/files/55543125/aoirethics2.pdf.
[24] UNESCO, *Global Media and Information Literacy Assessment Framework*. Paris: UNESCO Publishing, 2018. [Online]. Available: https://www.unesco.org.
[25] A. Mbembe, *De la postcolonie: Essai sur l'imagination politique dans l'Afrique contemporaine*. Paris: Karthala, 2000. https://books.google.co.id/books?id=VadCCBHLy68C.
[26] T. August, H. Shin, T. I. Tunca, "Licensing and Competition for Services in Open Source Software," *Information Systems Research*, vol. 24, no. 4, pp. 1068-1086, 2013. https://doi.org/10.1287/isre.2013.0486.
[27] J.-P. P. Kamili, R. M. Taghembwa, and J.-B. K. Mbakula, "Role of media in promoting peace and conflict resolution in North Kivu, Democratic Republic of the Congo," *Journalism and Mass Communication*, vol. 14, no. 2, pp. 101-111, 2024. https://doi.org/10.17265/2160-6579/2024.02.006.
[28] J. Muhindo Kavyavu, "Les incidences du numérique sur la famille : usages et appropriation dans les ménages de Goma," Mémoire de recherche universitaire, 2025.
[29] CIPESA, *State of Internet Freedom in Africa Report*. Kampala, Uganda, 2023. [Online]. Available: https://cipesa.org.
[30] Internews, *Digital Ecosystem Assessment for the Democratic Republic of the Congo*. Washington, DC, USA, 2022. [Online]. Available: https://internews.org.
[31] A. Mbuyu, "L'impact des réseaux sociaux sur le comportement des Congolais modernes : cas de TikTok," Mémoire universitaire, 2023. https://www.memoireonline.com/09/23/14290/Limpact-des-reseaux-sociaux-sur-le-comportement-des-congolais-modernes-cas-de-Tiktok.html.