GUIDELINES

FOR DIGITAL RIGHTS AND SAFETY BEST PRACTICES

NIGERIA

IMS

GUIDELINES

FOR DIGITAL RIGHTS AND SAFETY BEST PRACTICES

NIGERIA

With Support from

ifex

Published in 2022
By
Institute for Media and Society (IMS)
3, Emina Crescent, Off Toyin Street,
Ikeja, Lagos, Nigeria.
Email: info@imesoimeso.org
imesoimeso@hotmail.com
Website: www.imesoimeso.org

ISBN:

DISCLAIMER

This publication has been produced with the support of the IFEX.
The contents of this publication are the sole responsibility of the ***Institute for Media and Society,*** and can in no way be taken to reflect the views of the IFEX.

CONTENT

ACKNOWLEDGEMENTS

The publication of *Guidelines for Digital Rights and Safety Best Practices* is a strategic component of a project on *Strengthening Protection of Citizens' Online Rights and Building Capacity of Digital Rights Defenders in Nigeria* implemented by the Institute for Media and Society (IMS), Nigeria between October 2021 and November 2022. The grant support was provided by IFEX- The global network defending and promoting free expression.

We wish to thank IFEX, engaged consultants who worked on the development of the Guidelines- Messers Olumide Babalola and Jonathan Agbo (of the Digital Rights Lawyers Initiative), Dr Wole Oladapo of the Department of Communications and Language Arts, University of Ibadan, Nigeria; as well as participants and other stakeholders on the project. The efforts of the Project Team and Backroom staff at IMS who planned and implemented the project are highly valued and appreciated.

INTRODUCTION

Digital technologies used in information and communication fields emerged as boosters of democracy. They came with the promise of democratising access to information, thereby making the world a true global village. While they have truly been revolutionary in almost all aspects of information and communication, they have come with some challenges that are strong enough to neutralise all the benefits. The way human rights in the everyday society have been preserved and protected through concerted efforts is the same way human rights in the digital space, otherwise known as digital rights, can be preserved and protected.

Those who work for media organisations, whether hybrid or fully online platforms, are constantly a target of attacks in the digital space. Even bloggers and social media influencers are exposed to similar attacks. Those who design digital technologies like programmers and web designers could be victim and perpetrators of digital attacks depending on their intention and ethical orientation. Therefore, they need

protection as much as other actors need to be protected from them. The sources of the attacks could be isolated or coordinated. But without safety strategies for responding to exposure to such attacks, the digital space would be a dreaded place where only might is right.

Meanwhile, the challenges are not peculiar to those in the information and communication sectors. Digital technologies have found their way into almost all aspects of human life. The development comes with unprecedented challenges of diverse forms for various actors. Although the magnitude of the challenges varies for different categories of digital media users, the consequences could be equally devastating for all. Marginalized and vulnerable groups such as women, persons with disabilities, and children – both the boychild and the girlchild require deliberate acts of protection against certain threats that are targeted at them in the digital space.

However, until there is a universal declaration of digital rights by the United Nations and its adoption by member states, local efforts will continue to fill the gaps created by its absence. This guidelines publication is one of such efforts. Its primary objectives are to create awareness about the rights that media organisations, their workers, and all other actors have in the digital space; identify threats to those rights; and highlights how they can keep themselves and their information business safe in the digital space.

SECTION 1

CONTEXT: DIGITAL RIGHTS AND SAFETY IN NIGERIA

1.1. The Internet has made a lot of things possible. With a device and active subscription, what one cannot do on the Internet today is only left to the imagination. From making online purchases, to research, breaking news as they happen, tracking major economic development and governance issues, organizing advocacy events, creating wealth and employment, and advancing education, the opportunities made possible by the Internet appear limitless.

1.2. However, with the opportunities come many threats. Each day comes with major stories of data theft, privacy breach, theft of intellectual property, election meddling, internet pornography, and cybercrimes. Add to the list attempts to gag free speech online and restrict internet freedoms through censorships, the use of bots, trolls, and excessively restrictive regulations. It is safe to say that while the Internet has provided many opportunities for users worldwide, it has also brought with it many challenges that require constant action to mitigate and, in appropriate cases, eradicate those challenges.

1.3. The world over, regulators, businesses, and governments

need to take measures that ensure the security of users' data, protection of minors, prevention of online harassment, and gender-based violence, and at the same time enhance the protection of internet freedoms, chief among which is the right to freedom of expression online. There is also the need to ensure the creation and maintenance of an enabling environment for creation of and securing wealth and employment using digital means.

1.4. These have always required a balancing act because on the one hand, the excessive use of restrictive legislation and regulatory action has led to the restriction of internet freedoms in Nigeria. On the other hand, unregulated internet exposes users to the dangers highlighted and many more.

State of Digital Rights in Nigeria (December 2021 to August 2022)

Digital platforms such as Facebook Messenger, Telegram and WhatsApp were frequently inaccessible during the stated timeframe. Most of the blocks and internet disruptions in Nigeria between December 2021 and August 2022 occurred mostly in the North-East and North-Western regions. Notably, eighty per cent of the attacks that occurred in the Southern region of Nigeria were targeted at journalists and other types of digital assets such as blogs, and websites.

Institute for Media and Society (IMS) Digital Rights and Threats Monitoring Report (2022).

1.1. The media community has had its own fair share of concerns relating to digital safety and information integrity issues. Often and again, journalists, bloggers, media outlets and social media platforms grapple with data breaches, privacy violations, malware and ransomware attacks and arbitrary arrests for just doing their jobs. There is also the problem of lack or failure of institutional mechanisms to deal with the issues above.

1.2. This guideline addresses the above issues and provides relevant recommendations on practical steps that media practitioners can take to mitigate and eliminate risks to the integrity of data and close access gaps.

1.3. This guideline addresses some of the challenges facing internet freedoms in Nigeria with particular focus on challenges to information integrity and internet safety. It compares international best practices and makes recommendations that address these challenges.

1.4. It addresses specific threats to information integrity such as phishing, cyberbullying, use of bots and trolls online and on social media, disinformation and fake news, privacy violations and misuse of data and the measures to protect the integrity of information, address data and privacy breach/violation.

SECTION 2

DIGITAL RIGHTS

Key Digital Rights

1. Right to seek, receive, and provide information on digital platforms
2. Right to hold and express opinions on issues of public importance
3. Right to ownership of the information of diverse kinds
4. Right to restrict or prevent unauthorize access to personal and organisational information

Many organisations including media, business and civil society organisations have become significantly transformed from what they used to be in the pre-digital technologies' era. Many of those that were hitherto analogue have now gone hybrid in their information gathering and distribution processes while fully digitized organisations have emerged. Because of the centrality of digital technologies to their operations, organisations are expected to be conversant with the rights that producers of information on digital technologies enjoy and be aware of how to protect those rights from infringements.

Luci Pangrazio and Julian Sefton-Green define digital rights as "Human and legal rights that allow individuals to access, use, create and publish digital content on devices such as computers and mobile phones, as well as in virtual spaces and communities'.[1]

On the scope of digital rights, Media Defence (a UK based civil society) noted that:

"It is now firmly entrenched by both the African Commission on Human and Peoples' Rights (ACHPR) and the United Nations (UN) that the same rights that people have offline must also be protected online, in particular the right to freedom of expression…."

The term 'digital rights', therefore, comprises the rights that are embedded in our access to and use of these technologies. It also necessitates the consideration of what commensurate obligations there are on states and other actors to protect these rights."[2]

In other interventions, the concept of 'digital rights' has also been defined as follows: "Fundamental rights in the digital age';[3] 'human rights' that

[1] Luci Pangrazio and Julian Sefton-Green 'Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?' accessible at https://naerjournal.ua.es/article/view/v10n1-1 accessed on 15 September 2022.

[2] See Media Defence 'Training Manual on Digital Rights and Freedom of Expression Online' < https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf> accessed on 17 September 2022.

[3] See Igor Calzada, 'The right to have digital rights in smart cities' (2021) 13(20) Sustainability, 11438.

enable human beings to utilise, access, provide and create contents on digital platforms and virtual spaces'[4]; 'Freedoms afforded everyone in a digital space'[5]; 'Human rights in the digital environments'[6; The defence of freedom of expression, privacy, innovation, creativity, and consumer rights on the internet'[7]; 'Human and legal rights that allow individuals to access, use, create and publish digital content on devices such as computers and mobile phones, as well as in virtual spaces and communities'.[8]

It is for this reason that regulators and policy makers the world over make laws and policies that regulate the enjoyment of, and satisfaction of obligations that come with the enjoyment of digital rights. For example, Internet service providers and digital platform enablers make money from the services they render and have a concomitant duty tocomply with regulatory obligations such as having a privacy policy, appointment of data protection officers and ensuring robust cyber-security systems to prevent malware attacks and data breaches etc.9

[4] See Nani Reventlow, 'Digital rights are human rights. And you can defend them in court' < https://digitalfreedomfund.org/digital-rights-are-also-human-rights-and-you-can-enforce-them-in-court-too/> accessed 13 September 2022.

[5] Mathew N.O. Sadiku, et al, 'Digital citizenship' (2018) 8(5) International Journals of Advanced Research in Computer Science and Software Engineering, 18.

[6] Kathleen Azali, 'What are digital rights' (2020) <coconut –social/2020/digital-rights-exploring-definitions/> accessed 14 February 2022.

[7] Tamy Guberek and Romesh Silva, 'Human rights and technology: Mapping the Landscape to support Grant making' (2014) Prima Information Methodology and Analysis Report, 2014, 12.

8 Ibid.

[9] Stanislaw Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors' (2021) 43mComputer Law & Security Review, 105614.

The Nigerian courts are yet to expressly accord recognition to digital rights as fundamental rights and so, the legal landscape on the subject matter is still fluid. However, the courts have recognized various aspects of the exercise of digital rights. For instance, the right to control or keep personal data or information from unauthorised processing (use, storage, transmission, alteration etc) has been recognized as a constitutional right under right to privacy.[10]

The UN Declaration of Human Rights (UDHR) recognizes the need to enjoy on the Internet, rights also protected offline and provides for the recognition of amongst others, the right to freedom of expression online, data privacy and related rights.[11] Many countries of the world also make comprehensive provision for the enjoyment of digital rights, at least specific aspects of it, like the right to privacy, freedom of expression and data protection, open internet and these rights have been recognized as part of the jurisprudence in many counties especially the EU.

2.1. Types of Digital Rights

As stated earlier, the reference to digital rights includes the enjoyment online of any right that can be exercised physically. It follows that digital right is simply an expression of the rights that

[10] Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v. National Identity Management Commission (NIMC) (2021) LPELR-55623(CA)

[11] Universal Declaration of Human Rights, article 19. See also Catherin Cowelll, ' Internet as a human right' < https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/> accessed 16 September 2022.

accrue to a person in every endeavour. For this guideline, the digital rights include the following:

a. Freedom of expression online: the right to freedom of expression is a constitutionally recognized right in Nigeria and all over the world. The right to freedom of expression is a fundamental human right which is contained in article 19 of the Universal Declaration of Human Rights (UDHR) which states that: "everyone has the right to freedom of opinion and expression, the rights includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". The right to freedom of expression is also contained in Section 39 of the Constitution of the Federal Republic of Nigeria 1999. While the right to freedom of expression is generally accepted within the context of Nigeria's legal framework, the recognition of that right online is a relatively new jurisprudential issue that is being sought to be entrenched through judicial activism of digital rights advocates. This is reflected in the cases pursued in the strata of Nigerian Courts. The exercise of this right is essential for guaranteeing human rights, democracy, and the rule of law. Without free expression and free media, violations of human rights may remain hidden with the propensity to give rise to impunity and continuous violations.

B. Intellectual property: the expression of one's ideas and dissemination of information using electronic media generally comes with the exertion of one's intellect. This in turn leads to the creation of intangible assets that are capable of being owned and exchanged for value. these assets are called intellectual property. They come in various forms and include such things as artistic impressions, drawings, and Non-fungible Tokens (NFTs). Media contents of various types,

including news stories, images, and cartoons, enjoy intellectual property rights. The rights are protected by different legal regimes. For instance, the right to content, artistic impressions, cinematographic items, sound and their modifications are protected by copyright while trade or service marks created exclusively to protect and create distinction in one's work are protected by trademarks. In other circumstances, these rights are protected by a combination of legal regimes. Other aspects of intellectual property not codified but which enjoy protection nonetheless include trade secrets.

C. Data privacy: This refers to the right to keep and maintain the integrity of and prevent unauthorized access to one's personal data. The principal regulation that protects data privacy in Nigeria is the Nigerian Data Protection Regulation 2019. In addition, individuals and institutions have sought to enforce data privacy rights against breaches by government and other institutions in Nigeria through judicial activism.

While there is some level of internet freedom in Nigeria, statistics show that the recognition and protection of digital rights is not a straightforward matter. Nigeria is regarded as a country with partial internet freedom and her citizens often experience violation of users' rights from data privacy breach by state actors, cyberattacks against private and public database, repression of freedom of expression online, and the misuse of laws to stifle dissent and civic engagement.[12]

[12] https://freedomhouse.org/country/nigeria/freedom-net/2021 accessed 13 September 2022.

Other challenges to internet/digital rights include poor internet penetration, lack of rural access/inclusion and prohibitive cost. These challenges impair the enjoyment of digital rights in Nigeria. Ultimately, although understanding the concept of digital rights has been restricted to online expression and data privacy in some quarters, its reach is wider enough to accommodate all legal rights exercisable on the Internet or digital platforms.[13]

There is no gainsaying that media practitioners enjoy a lot of digital rights. Newspapers, blogs, digital news channels all create content that carry digital rights with them. For example, inherent in every breaking news is copyrights owned by the maker. Again, the use of electronic channels creates opportunities to make and own trademarks and the right to control the use of these Intellectual property rights. And with these rights come the challenges to information integrity. Digital rights for media practitioners also include online expression, privacy, and the right to control access to information otherwise known as data protection.

[13] For example, intellectual property rights, consumer rights, digital rights management etc. See Kari Karppinen, 'Four Discourses of Digital Rights: Promises and Problems of Rights-Based Politics' (2020) 10 Journal of Information Policy, 304-328

SECTION 3

DIGITAL SAFETY

Digital Safety Measures

1. By government and regulators: laws and regulatory codes

2. By service providers: standards and operational procedures

3. By client: constantly reviewed and updated, fully implemented internet safety policy complemented with investment in safety technology, and building of organization-wide cybersecurity culture of strict compliance

4. By individuals: digital literacy and compliance with safety protocols

The Internet is described as information superhighway. Just as it is with the physical highway, issues of safety abound on the Internet too. In its simplest form, Internet safety [14] refers to the awareness of the dangers of using the Internet and the methods deployed to mitigate the dangers or prevent them from occurring. Internet safety has also been defined as 'a set of issues that are, either directly or indirectly, related to the physical and psychological well-being of Internet users.' [15] Any compromise to internet safety limits the extent to which digital rights could be enjoyed.

[14] Also referred to as digital safety, online safety or e-safety.

[15] Lies De Kimpe, 'Internet Safety' < https://www.researchgate.net/publication/332989526_Internet_Safety> accessed 16 September 2022.

Internet safety is generally enhanced by a number of individual/personal, technical and regulatory measures – all with an overriding objective of securing computer devices or networks.

Cybersecurity refers to the methods and processes designed to keep users safe online and to protect devices from malwares. Online safety means the awareness of those processes and using them to stay protected. As the number of persons who use internet services increases exponentially so does the risk involved. Reports indicate that about 63.1 % of the world's population, representing 5.3 billion people use the Internet. Of that number, 4.70 billion people use social media actively.[16] Statista reports that 51% of Nigeria's population accesses the Internet with mobile internet penetration accounting for 84% of such use.[17]

The record shows a massive use of the Internet the world over and as the number of users increase, so do the attacks. For example, a survey in 2021 revealed that 3 of every 5 companies in

[16] https://datareportal.com/global digitaloverview#:~:text=Internet%20use%20around%20the%20world,million%20new%20 users%20every%20day.

[17] https://www.statista.com/topics/7199/internet-usage-in-nigeria/#topicHeader__wrapper

the supply chain industry suffered a malware attack.[18] Another report showed that the total number of data breaches and ransomware attacks increased by 15.1% in 2021 from 2020.

The reports show the need for awareness of the dangers that users of digital services face. They also underscore the importance of awareness of internet safety measures and the need to deploy them effectively in order to stay protected.

Staying safe online requires a mix of regulations and actions from stakeholders such as companies and governments.

In Nigeria, the apex communications regulatory body, the Nigerian Communications Commission, has issued several codes and publications to protect users and make internet service providers (ISPs) accountable in the event of breach. For example, the Internet Code of Practice[19] provides for the security of users' information thus

"An Internet Access Service Provider shall take reasonable measures to protect customer information from unauthorized use, disclosure, or access. The security measures taken by an Internet Access Service Provider to implement the requirement set forth in this section shall appropriately take into account each of the following factors; I. The sensitivity of the data collected; and II. Technical feasibility."[20]

[18] https://www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Software%20supply%20chain%20attacks%20hit%20three%20out%20of%20five%20companies%20in%202021&utm_campaign=CSO%20US%20First%20Look&utm_term=CSO%20US%20Editorial%20Newsletters&utm_date=20220219174907&huid=040100f5-bc13-4688-af2b-08a56480a80e

[19] Nigeria Communications Commission Internet Code of Practice 2019.

[20] Article 4.2.

In the event of data breach, the Code further mandates ISPs to make proactive disclosure to user thus: "An Internet Access Service Provider shall notify affected customers of any breach relating to the customer's information within 48 hours of its occurrence, by email and text message."[21]

The imposition of regulatory obligations creates a mandatory requirement on ISPs and social media platforms to take action that protect users online. It keeps users safe from harmful activity like stalking, information theft and malware attacks which will be discussed in detail in Section 3.

For media practitioners, internet safety or digital safety is a constant concern. Journalists, for example, make news and in today's environment, traditional journalism has taken a back seat. News can be published either from a multi-million-dollar newsroom or from the bedroom corner. In either case, the making or breaking of news puts journalists in challenging situations as oftentimes, the news they break either challenges power or leads to the revealing of otherwise kept secrets. The use of electronic means makes this even more challenging.

Because of the possibilities that the Internet offers, both professionals and untrained persons create news content today. This creates a problem of ethics. Again, the proliferation of persons who create news content increases the risk for digital stakeholders like journalists, especially by those who seek to control news and its dissemination. This leads to hacking, online attacks, indiscriminate arrests and detention, disinformation attempts through robots and online trolls who seek to discredit otherwise

[21] Article 4.3.

credible information and as now become the case, journalists face the risk of death arising from internet use. These constitute threats to internet safety that must be constantly addressed for a safer work environment.[22]

SECTION 3.1.

How to Avoid Threats to Information Integrity

1. Ensure that all data sources are integrated, and that each member of staff adheres strictly to the integration procedure

2. Avoid manual data entry and collection process as much as possible. Instead ensure that information is shared via the organization's networked computer system

3. Adopt a uniform data analytics tool for the organisation.

4. Ensure a professional, constant, and consistent information audit procedure.

5. Subscribe to new versions or editions of computer programme and application software and keep them up to date. Free versions may expose you to diverse forms of attack.

6. Invest in data security and maintenance.

7. Clearly define how data is collected, stored, and used within the organisations, highlighting the responsibilities of each member of staff in the process.

[22] Jennifer R. Henrichsen, etal (2015) Building Safety for Journalism: A survey of selected issues, UNESCO publishing, https://unesdoc.unesco.org/ark:/48223/pf0000232358, accessed on the 22nd, September, 2022

3.1 Information Integrity

Information in this context refers to 'an item of information or intelligence; a fact or circumstance of which one is told', 'stored knowledge.'[23] Boell et al define information as 'processed data' that is endowed with meaning, e.g.: "Information is processed data that is meaningful'[24]

Information integrity, therefore, entails preserving the accuracy and completeness of information. Information is trustworthy only when its integrity is preserved. Information that has been tampered with cannot pass the test of information integrity.

The integrity of information is central to smooth operation of a media organisation. This is quite important because media organisations deal in information. The reputation of a media organisation depends largely on the trust that the public have in the information that the organisation provides.

As a result, media organisations must be confident that the information they supply to data controllers are not only safe but are preserved in the best possible way. They must also be confident that digital platforms or ISPs comply with regulatory and statutory obligations in their data management practices. This is integral to the protection of digital rights.

[23] A.D. Madden, 'A definition of information' (2000) 52(9) Aslib Proceeding, 343

[24] Sebastian Boell, 'What is 'Information' Beyond a Definition?' Thirty Sixth International Conference on Information Systems, Fort Worth 2015 < https://www.researchgate.net/publication/285581995_What_is_'Information'_Beyond_a_Definition> accessed 16 September 2022.

3.2 Threats to Digital Safety

Multiple challenges occur when an institution or business lacks effective data integrity policy or practice and encounter problems as a result. A number of issues impact businesses and digital activities vis a vis data integrity concerns as follows:

a. Lack of data integration: This is a technical term defined as 'degree or presence in a vertical relationship of hierarchy-like mechanisms that are informational in nature'[25] Stakeholders' analysis shows that as an organization's data sprawl grows, it becomes increasingly difficult to meet the demands for accurate and consistent data.[26] Often, data isn't where it should be or sometimes, it's late getting there. There are also cases of data duplication or incorrect formatting of data. Each of the above scenarios is said to represent a lack of data integration and leaves users to question the trustworthiness of data.

b. Manual data entry and collection processes: Manual processes are inherently error-prone and are the root cause of many data integrity issues. Therefore, eliminating as many manual processing of data as possible should be mission-critical for organizations. Implementing data validation processes restricts the data values users can enter into a cell, in an effort to eliminate input mistakes. Examples include text or data field types, drop-

[25] Ricardo M. Checchi, 'Digital integration: Understanding the concept and its environmental predictors' (2008) < https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1024&context=cis_diss> accessed 16 September 2022.

[26] ???

down lists, and multiple-choice menus. Deploying data validation across an enterprise can be daunting and never-ending, though, without the right approach.

c. Multiple analytics tools: Institutions and news media establishments that have operated over time have a strong chance of having accumulated multiple analytics tools for different functions within the organization. Without a properly synchronized communication method, these analytic tools lead to conflicting results. Data integration efforts and an effective technology stack will eliminate siloed analytics by standardizing data access and analysis across the organization. The deployment of various analytic tools to synchronize efforts make the job easier.

d. Poor auditing: Knowing the "who, what, when, where, and why" of every change is essential for data integrity. Without complete and consistent audit trails, there's no way to ensure accurate and trustworthy data. A data steward or data controller can provide oversight, monitor audit trails, and take appropriate corrective action when necessary.

e. Reliance on legacy systems: Despite advances in technology, some organisations still rely on outdated data management techniques such as traditional enterprise data warehouses (EDW) or Excel spreadsheets. Of course, these legacy systems do not support data integrity or sophisticated analytics. Modern, data-driven organisations leverage the cloud to unify their data where it can be accessed for analysis and business intelligence.

f. Deficient data entry skills: When handlers of personal data aren't properly trained on data integrity policies and processes, they're likely to introduce errors into users' data that could potentially impact the entire

organisation. Regular training reinforces best practices for how users should interact with data, helping to minimise errors. Training also promotes the idea that everyone is accountable for data accuracy and data quality, ensuring users feel invested in the organisation's overall data integrity.[27]

g. Inadequate data security and maintenance: Along with human error, inadequate security and maintenance practices also contribute to data integrity issues. Staying up to date with antiviral software and current security threats while constantly monitoring and adjusting data access controls are essential to maintaining overall data integrity.

H. Data governance: This refers to how an organisation leverages its people, processes, and technology to manage its internal data. This is done by simply creating a framework or template which are specific set of principles and processes that defines how data is collected, stored, and used within an organisation. With the proper framework in place, organisations can transform their data into a valuable, powerful asset that can be leveraged to meet or exceed the business' goals and objectives. At a minimum, a data governance framework should establish the following policies for each data asset in the organisation: Structure, Access, Usage, Classification, and Integrity.

The challenges identified above are all problems that affect the integrity of data, impact the protection of digital rights and worsen the digital divide among media practitioners and for users

[27] https://www.claravine.com/fix-these-7-data-integrity-issues-and-embrace-best-practices/

generally. It only follows that resolving them mitigates the threats and increases efficiency in data management and access control options.

Section 3.3 Attacks on Digital Safety

1. Cyberbullying and cyberstalking

2. Phishing

3. Defamation

4. Cyber-surveillance abuse

3.3 Attacks on Digital Safety

The point had been made earlier that digital rights come with varying degrees of challenges that impair the enjoyment of those rights. This part focuses on some of the risks associated with digital rights the world over.

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable illicit activity. Computer crime mainly consists of unauthorised access to computer systems, data alteration, data destruction, and theft of intellectual property. Cybercrime in the context of national security may involve traditional espionage, or information warfare and related activities. Elements of cybercrimes also include cyberstalking, hacking or unauthorised access

and within the Nigerian context, it includes such things as unlawful interception, tampering with critical infrastructure, wilful misdirection of electronic messages, fraudulent computer activity and computer forgery, amongst others. It is a global issue that affects the smooth functioning of governments, businesses, and private life. Emerging threats like cross site scripting and vishing already affects lives and businesses across the world.[28] In Nigeria, cybercrimes carry varying degrees of sanctions from hefty fines to long imprisonment terms and forfeiture of property.

Cyberbullying and cyberstalking: In its broad form, cyberbullying[29] involves harassment using online/digital means such as instant messaging apps (Facebook, WhatsApp), emails, and online chat rooms. It is a "deliberate and hostile behaviour by an individual or a group of individuals that involves using SNSs to repeatedly communicate aggressive content intended to inflict harm or discomfort on a target"[30]

Perpetration of cyberbullying has been reportedly easy and rampant because of the nuances of online communications. Unlike physical communication, engagements online usually

[28] V. Karamchand Gandhi , (2012) ,An Overview Study on Cybercrimes in Internet , Journal of Information Engineering and Applications, www.iiste.org ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.1, 1

[29] Also referred to as 'Internet bullying, electronic bullying, Internet harassment, online bullying etc. See Robin Kowalski, Cyberbullying: Bullying in the digital age (Wiley Blackwell, Publishing 2012).

[30] Tommy Chan, 'Cyberbullying on social networking sites: A literature review and future research directions' (2021) 58 Information and Management,

means that users are hidden behind devices such as computers, tablets or phones and cannot be 'seen'. The restrictions or constraints that physical conversations carry with it are therefore absent. As a result, cyberbullies are left mostly unrestrained.

There is also disagreement as to at what point insults online becomes illegal. In the USA, generally, unless it involves the threat to life or imminent danger, cyberstalking or harassment, cyberbullying is mostly not considered illegal.[31] In Nigeria, section 24 (1) and (2) of the Cybercrime (prohibition, prevention etc) Act specifically prohibits cyberstalking. In defining the specific situations that constitute cyberstalking however, 24(2) (a) include words like "threaten, bully, and harass another person" but adds a qualification that such words must place the victim in fear of death, bodily harm or violence. The implication of the above is that like the USA, cyberbullying will constitute an offence only if it amounts to harassment or causes fear or apprehension to the victim.

It follows that cyberbullying, in all its forms, is considered, at the very least, a negative activity that can amount to criminal offences. Cyberbullying is considered as a stressor and contributes to negative

[31] Charles E. Notar, Sharon Padgett and Jessica Roden (2013), Cyber Bullying: A review of Literature, Universal Journal of Educational Research, Vol 1 (1), DOI: 10.13189/ujer.2013.010101. accessed 15th September 2022.

tendencies including loneliness, delinquent behaviour and depression.[32]

Phishing: This is one of the means through which online fraud is perpetuated. Phishing refers to the receipt of unsolicited emails by users, especially customers of financial institutions, requesting them to enter personal information through which their accounts are accessed such as passwords and credit card, social security, and bank account numbers, that the legitimate organisation already has. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. For example, 2003 saw the proliferation of a phishing scam in which users received emails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a website look like a legitimate organisation's site by mimicking the HTML code, the scam counted on people being tricked into thinking they were being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the email being read by a

[32] Nixon CL. Current perspectives: the impact of cyberbullying on adolescent health. Adolesc Health Med Ther. 2014 Aug 1;5:143-58. doi: 10.2147/AHMT.S36456. PMID: 25177157; PMCID: PMC4126576.

percentage of people who had listed credit card numbers with eBay legitimately. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.[33]

While phishing is not a new type of fraudulent activity, the pandemic saw a rise in phishing activity in 2020, rising as high as 102% between July and September of that year. Phishing activity was notable in sites mimicking official websites providing health related information during the pandemic.[34] Audience of media organisations that hide their contents behind paywall might fall victim to phishing. This is one of the reasons that media organisations must put measures in place to protect its data from cyberattacks.

Defamation: Generally, defamation is the act of injuring a person's character, fame or reputation by false and malicious statements. Defamation is the general term that is commonly categorised as either libel or slander. Libel is a written defamation while slander is verbal defamation. It falls under the Law of Tort and a broader legal definition of the concept refers to false statements about a person communicated as fact to one or more other persons by an individual or entity (such as a person, newspaper, magazine or political organisation), with the malicious aim of causing damage to the victims' reputation.

The effect of defamation is to generally lower the victim's esteem in the

[33] ibid.

[34] Https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-lis

eyes of persons close to him or to expose the victim to public odium. Defamation can be carried out both offline and online. For instance, when a person spreads malicious gossip about another verbally, it is called slander and if the malicious information is put into writing, it constitutes libel. Both activities can be carried out online either by posting information through instant messaging, emails, online articles, or voice enabled publication like the use of voice notes on social media platforms.

It simply means defamation through online activity where false statements are written or published through online mediums with the aim of harming the target's reputation or standing online. The written words are usually negative and generally false. The striking feature here is that other online users on the internet may see the messages or publication and could spread the word faster than if the perpetuator spoke the information to just a friend or crowd. Thus, this specie of defamation could cover a wider range of locations and areas of the country or world than a usual defamation claim. Defamation through online use and spreading false statements through web content has become a problem in the age of the computer.

Defamation should be a serious concern to key actors in the civic and political expression e.g. media organisations. The reason is that the media can be a victim and a perpetrator of defamation, the latter being the more common. When media organisations engage in acts of defamation online, the violate the rights of their victims to dignity and respect in the digital space.

With an internet enabled device like a smart phone or computer, it

is easy to type and send false and defamatory information about a victim and spread same across great distances and reach an even unintended audience. Caught up in the race to break the news, the media can fall easily into publishing defamatory content online if care is not taken. There is generally the agreement that digital rights promote free speech. However, the line between free speech and defamation is so thin that many regulators insist on censorship at the expense of free speech. In Nigeria, for example, attempts have been made to promote censorship in the form of regulations that permit law enforcement agencies to access or demand information about online activity without a user's knowledge. These regulations have raised concerns about freedom of expression online and have formed the basis of judicial activism on defence of free speech.

Cyber-surveillance attack: Media organisations and journalists are often victims of illegal cyber-surveillance conducted with the aid of sophisticated technologies. Dictatorial regimes as well as democratic governments have been found to engage in acts of illegal surveillance of citizens. This is a big threat to media organisations because of the nature of their operations. Through illegal cyber-surveillance, organisational and personal data can become compromised, an act which violates digital rights to privacy. In the process, the identities of some sensitive anonymous media sources might be revealed, exposing them to different degrees of harm. This is a real threat for the Nigerian media as it is established that the Nigerian governments over the years have invested

significantly in surveillance technologies.[35]

Generally, there is a connection between all threats or dangers that come with digital rights such that in most cases, all that is simply required is an effective integration of processes that mitigate them.

3.4 : Agenda for Digital Safety Advocacy

The penetration of digital technologies into all aspects of societal life, both private and public, makes issues in digital safety pervasive. To make digital technologies serve the needs of society, concerted efforts are needed from different stakeholders. Especially activists and civil society organisations have an important role to play in advocating for the digital safety of specific groups of people and in ensuring that those who have policy power use it to create a digital space that is safe for all. This section of the guidelines considers the digital safety needs of especially vulnerable groups and the digital safety responsibilities of policy and technical groups.

Media

Policy threats: Government increasingly introduces policies that allow mandated internet disruptions, and arbitrary sanctions such as fine, and take-down orders. Freedom of information and expression cannot be ensured where media-unfriendly policies

[35] Oladapo, O., & Ojebode, A. (2021). Nigeria Digital Rights Landscape Report. Digital Rights in Closing Civic Space: Lessons from Ten African Countries. https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15964/Nigeria_Report.pdf

thrive. Digital rights and safety advocates must constantly engage policy makers to identify aspects of proposed laws and policies that may endanger the media and their operations and collectively produce alternatives which serve all parties better.

Security threats: The media are often a target of diverse forms of cyberattacks. They could experience corporate identity theft with their websites and other digital platforms such as social media accounts cloned by cybercriminals to perpetrate criminal acts. Media organizations need constant capacity building alongside investment in technology to be able to withstand sophisticated online security threats.

Economic threats: The media have not been able to develop a sustainable means to monetize their digital contents without restricting access to only those who can pay for it. They are caught in the middle of either hiding their contents behind pay walls and losing a large part of their audience or upholding the access-for-all model and continue to struggle to sustain their businesses. Sustained engagement with media owners and workers is important to developing media business models that are profitable and yet preserve digital rights of the audience and are responsive to the peculiarities of the digital media environment.

Women

Gender-based attacks: Women are constantly exposed to various forms of harassments, victimization, stereotype, blackmail, stalking, and body-shaming, purposeful embarrassment, and even threats of physical attacks in online spaces. Responsive systems for protecting women from cyberattacks need to be instituted through the collaboration of relevant stakeholders.

Paucity of gendered online safe spaces: Women have limited access to safe spaces where they could meet and discuss without fear issues that are of interest to them as individuals and as a group. As a result, they have limited chances of speaking up and seeking redress when they suffer abuses and violations online. Digital safe spaces for women need to become a priority to fully included women in the digital world.

Adaptive safety measures: Many online safety measures do not take into consideration the peculiarity of women's online needs and experiences. Women need online safety measures that are adaptive to both their needs and experiences in the digital space.

Persons with Disabilities

Accessibility: Although international best practices in digital technology design take cognizance of disability inclusion, compliance among local developers is still low. Also, the concept of disability inclusion in digital technology design needs to be inclusive to cover all existing types of disability.

Personalized usability information: Digital products information often ignores the peculiarity of the needs of persons with disabilities. They hardly adapt the information to those needs, leaving persons with disabilities unable to fully maximize the benefits of the technologies.

Adaptive protection against internet fraud: Cybercriminals often take advantage of the vulnerabilities of persons with disabilities to infringe of their digital rights and violate their digital safety. To keep safe on digital platforms, persons with disabilities often

require some additional layers of protection measures. Measures against internet fraud and other forms of cybercrimes should be adapted to the needs of persons with disabilities.

Tech Community

Tech community has a great role to play in ensuring the safety of users of digital technologies. Activists and civil society organisations must constantly engage them on how to bridge the gap that exists between digital technology innovations and safety of users of the technologies. Advocacy efforts must be devoted to the following important issues concerning tech community.

Ethical compliance: Digital technologies should be certified for ethical compliance before they are released to the public. They should not be such that infringe on digital rights of users or such that compromise their safety. International standards and best practices guiding ethical conducts in tech communities need to be domesticated and adapted to local realities to serve local users best.

Local adaptability: Designs, contents, and language of digital technologies should respond to the needs and attributes of the people that they are made to serve. The technology community needs to be constantly reminded of this important requirement.

Safety compliance: Digital technology designers must ensure that they provide up-to-date security information and measures about their products; alert users of their products to breaches and security threats as they are identified; release updates promptly to address security challenges; put in place a feedback channels through which users can report security challenges; and use user experience feedback for product

improvement.

Security policies: Digital technology companies must display strict compliance with relevant local and international laws and policies on digital safety and security and data protection. Efforts should be made to ensure that product are accompanied by a reader friendly and easy to understand version of the technical product policy agreements that are the norm.

Partnership for digital safety: The digital technology community must be a part of efforts to curb online violations and victimization of users.

Bloggers/social media influencers

Bloggers and social media influencers have come to wield an enormous amount of power that they can no longer be ignored. As much as bloggers and social media influencers need similar protection as the media and media workers, the public equally needs to be protected from bloggers and social media influencers. The following are areas where bloggers and social media influencers need to make constant improvement to be able to serve society well.

Professionalism: Bloggers and social media influencers need to be held up to a high standard of ethical compliance in their information creation and dissemination.

Knowledge of digital rights: Bloggers and social media influencers need to know what digital rights are, when they are violated, and how they can be protected. The knowledge will

enable them to protect themselves and to serve society better.

Children

Children are a vulnerable group. They are as vulnerable online as they are offline. Therefore, efforts being made to keep children safe offline must be extended to online as well. Below are measures to keep children safe on digital platforms.

Childproof technologies – Digital technologies meant for the use of children must be childproof. That is, the features of the technologies must be adapted to children's needs and attributes.

Protection from dangers – digital technologies should offer children protection from harmful contents and contents that are not age appropriate. It is established that merely rating especially contents on digital platforms does not prevent children from accessing them. Restrictions that require the help of an adult to bypass must be a feature of digital technologies that are designed with safety in mind.

Protection against cybercrime – Some cybercriminals purposefully target children with cybergrooming, cyberstalking, cyberbullying, and other forms of cybercrime. Children need to know the signs of these dangers and be equipped with appropriate response strategies.

Legal protection: The Child Rights Act needs to be amended to accommodate the digital rights of children and prioritize their safety in the digital space. This is the more important as children now spend an increasing amount of time on digital platforms due to widespread implementation of electronic learning.

SECTION 4

PROTECTION MECHANISMS

Digital Protection Mechanisms

1. Put in place an overall cybersecurity policy
2. Establish detailed data protection policy
3. Invest in cybersecurity infrastructure
4. Promote organisation wide digital literacy
5. Motivate employees to comply with information security protocols
6. Mainstream information audit into everyday organisational processes

The preceding parts of this publication focus on digital rights and its various ramifications, the threats to digital rights and emerging issues. This part focuses on application of cybersecurity measures to keep users safe on the Internet.

Cybersecurity as earlier defined, is the application of processes to protect systems, devices, and programs from attacks. Its importance cannot be overemphasised. As earlier noted, cyber threats are on the rise and are becoming increasingly sophisticated, leading to loss of critical data and undermining information integrity that results in loss of billions of dollars every year. In addition to the economic loss that cyber threat causes, it puts

the survival of many organisations, businesses and even governments at risk. A typical situation is the lawsuits that financial institutions and other organisations that handle a lot of data face over the loss or compromise of data.

A robust cybersecurity policy will necessarily include the adoption of a combination of physical and technical mechanisms such as access protocols which include safely securing devices and restricting unauthorised access among staff and from strangers; auditing which is the process of recording and checking events to detect whether any unexpected or unauthorised activity has taken place, or whether any attempt has been made to perform such activity, authentication protocols such as a set of protocols that control access to devices e.g the use of passwords and multi-step login procedures, and data encryption which prevents information from being read or readable in the event of breach. Employee training on the need to practice secure behaviour when handling data and a strong policy on information management also forms part of the process.

For practitioners, it is necessary to develop both on a personal and at organizational level a robust security practice that prevents unauthorized access to data or information, prevents the dilution of or tampering with data disseminated and protects the privacy of organizations and end users while allowing access in a safe and user-friendly manner. The specific cybersecurity measures are hereby addressed.

a. Data Protection: Personal data is as any information relating to an identified or identifiable natural person.[36] In similar but broader terms,

[36] Article 4(1) General Data Protection Regulation (GDPR)

the Nigeria Data Protection Regulation 2019 (NDPR) defines personal data as "any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.'

Across the world, the protecting of personal information collected under any of the available lawful bases[37] is considered as integral to the regulatory compliance and standardisation of any institution and stakeholders advocate a mix of mechanisms that ensure this very goal.

A good place to start as far as data protection is concerned is access control. It is generally agreed that an important requirement of any information management system is to protect data and resources against unauthorized disclosure, modifications, use and protecting against theft. Ensuring protection of personal information entrusted with any entity therefore requires that every access to a system and its resources be controlled and that all and only authorised accesses can take

[37] The NDPR, in no particular order recognises the following lawful bases: performance of contract, consent, vital interest, public interest and legal obligation.

place. A robust access control system will require the definition of the regulations according to which access is to be controlled and their implementation as functions executable by a computer system.

The development process is usually carried out with a multi-phase approach based on the following concepts: **Security policy** which defines the rules according to which access control must be regulated, **Security model** which provides a formal representation of the access control security policy and its working and **Security mechanism** which defines the low level (software and hardware) functions that implement the controls imposed by the policy and formally stated in the model.[38] It is advisable that in the design of the policy, mechanism and model, there is room for flexibility. This allows for an efficient operation of control mechanisms under different policies or models for if a mechanism is tied to a specific policy, a change in the policy would require changing the whole access control system while mechanisms able to enforce multiple policies avoid this drawback.

The Nigerian Data Protection Regulation also mandates that data can only be processed with the consent of the owner otherwise called Data subject. It follows that organisations who process third party data must not only ensure that consent is sought and obtained before processing data but must have a clear and adequate data policy in place. Staff or employees must understand the organisation's data policy and there should be constant training and update of staff and policy on compliance.

[38] Samarati, P., de Vimercati, S.C. (2001). Access Control: Policies, Models, and Mechanisms. In: Focardi, R., Gorrieri, R. (eds) Foundations of Security Analysis and Design. FOSAD 2000. Lecture Notes in Computer Science, vol 2171. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45608-2_3.

Compliance requirements also involve that organisations have data processing officers in place. A data processing officer is responsible for access, quality control and management of data. Such an officer must have sound knowledge of compliance obligations and must keep up to date with international best practices.

b. Information security: knowledge of information security is integral to the protection of an organisation's data. Lack of information security knowledge has been attributed to a number of factors including poor or lack of employee/staff engagement when designing information security policies, poor or inadequate understanding of roles within the framework of already designed policies, poor motivation of staff, including lack of training to act securely when handling organisation data. These issues affect the safety and integrity of information.

A major way to address this problem is by the development of information security knowledge sharing systems within organisations. It refers to the development of techniques or processes by which an organisation defines processes regarding the sharing of information and knowledge about organisation policies that protect critical data/information assets. Put differently, it means the development of knowledge sharing practices among employees, designed to protect data. A successful information sharing practice will require the total buy in of top management in every organisation as they allocate resources for such knowledge sharing activities.[39]

[39] Farkhondeh Hassandoust, Maduka Subasinghage, Allen C Johnston, (2022) A neo-institutional perspective on the establishment of information security knowledge sharing practices, Information & Management, Volume 59, Issue 1. https://doi.org/10.1016/j.im.2021.103574.

Also, a key area in information security management is discovering ways to motivate employees to engage in more secure behaviours. It is therefore recommended that from the start, employee background checks are important to ascertain criminal records, character, and fitness of the employee to handle sensitive data. This is primarily the function of the Human Resources department of an organisation but equally necessary is the development of a data/information security centric employment policy.

c. Internet education, otherwise known as digital literacy, is the ability to define, access, manage, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies and networked devices for participation in economic and social life. It includes competencies that are variously referred to as computer literacy, ICT literacy, information literacy, data literacy and media literacy. It prepares users for today's world of advanced technology and the future of work. Nigeria faces a number of challenges in relation to digital literacy such issues as failure of policy Implementation, educational curriculum that does not accommodate digital literacy skills, high cost of infrastructures such as the Internet and power, low rate of capacity building exercises and training on digital literacy across sectors and high exclusion rate among users are among such factors. For media practitioners, the point had been made earlier that a threat to information integrity is the incursion into the journalism space by untrained professionals. The ease with which the internet facilitates access to information and its dissemination also means that almost anybody with access can spread content.

The challenge this poses is the spread of fake news or disinformation. It also obfuscates readers and erodes confidence in online content. Stakeholders have suggested the establishment of professional bodies

for online journalists which allows the monitoring of content dissemination and facilitates proper training. Also, digital literacy skills with a particular reference to maintaining the integrity of data is recommended for practitioners while collaboration with relevant agencies to exploit existing provisions in regulations that seek to protect the integrity of data will prove effective. In this regard, the focus should be on providing necessary training on safe practices and imbibing safe behaviour online.

d. The following actions can also be undertaken by practitioners to address most of the issues:

i. More citizen engagement and awareness of existing and new policies on digital literacy

ii. Investment in research and development international best practices as it concerns promoting digital literacy

iii. Development of a digital literacy centric curriculum for practitioners through continuous education programs and professional training with special focus on information integrity systems and practices

Iv. Investment in digital infrastructure to bridge the digital divide

These steps, though not exhaustive, will also consider the need for monitoring and evaluation or constant review to determine the success of any such intervention and making adjustments in deserving cases. It is also recommended that expert opinion is collated in taking these interventions and attention must be given to localising actions for effective and wider reach.

CONCLUSION

This guideline has identified some specific aspects of digital rights, including the right to freedom of expression online, data privacy, intellectual property and data protection. It has also identified the most common challenges to information integrity and the means to mitigate them. The importance of establishing a robust data governance strategy, employee motivation to comply with data governance policies and the constant update of security measures have also been identified. The recommendations provided under each head in this guideline require constant review and update if it is to cover emerging threats and address the challenges posed to digital rights both by the practical application of the rights and the unintended consequences of the enjoyment of those rights. For effective results, it will also require a combination of partnerships with regulators and industry providers for implementation. They will however achieve tremendous results in bridging the knowledge gap, mitigating risks to the enjoyment of digital rights and the risks associated therewith.

1.1. DEFINITION OF TERMS

The following words have the meaning ascribed to them in this guideline unless otherwise indicated:

Bots: robots or software applications designed to simulate human activity without human intervention

Cyberattacks: attempts to gain unauthorized access to devices, systems, programs or data to cause damage

Cyberbullying: use of digital or online means to intimidate, harass or annoy users online typically through offensive messages

Cybercrimes: the commission of crime using computer devices and or via the internet

Cybersecurity: the application of technologies, processes, and control to protect systems, networks, devices, programs, and data from cyberattacks

Cyberspace: a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Cyberstalking: the use of the internet or other electronic media to stalk or harass an individual, group of persons or an organization

Cyber-surveillance attack: illegal collection of sensitive individual and organisational information through sophisticated software programmes

Ransomware: a type of malicious software designed to block an individual's access to his or her computer until an amount of money demanded is paid

Malware: a software designed to gain unauthorised access to a computer or system or disrupt its smooth operations

Data privacy: the protection and control of personal information from unauthorised access, use or utility

Data protection: the implementation of appropriate administrative, technical and physical measures to prevent unauthorised, accidental or intentional access to data/information

Disinformation: the intentional dissemination of false information with intent to mislead, confuse or manipulate data online

Digital rights: the aggregate of legal and human rights exercisable on the Internet and/or other digital platforms

Fake news: news that is intentionally written to mislead the reader, but which can be verified to be false

Information integrity: the overall accuracy, completeness, and consistency of data in compliance with regulatory frameworks

Internet safety: the understanding of and following actionable guidelines to protect digital devices and defend against online threats

Phishing: the fraudulent use of communication to obtain personal data that a data subject will otherwise not make available

Social media: a group of Internet-based applications that build on the ideological and technological foundations of the Web 2.0, which allows the creation and exchange of User Generated Content

Troll: a person or group of persons who use offensive posts on social media to cause disaffection, anger, or discomfort to other users

IMS

ifax