

OPEN ACCESS

*Correspondence

Olamide Emmanuel ABE

Article Received

18/06/2026

Accepted

24/06/2026

Published

06/07/2026

Works Cited

Olamide Emmanuel ABE, Hameedat Boluwatife ADEAGBO, Aondona, Precious Msendoo, AWOSEJO Oluwagbohunmi Abigeal., (2026). Cybersecurity and Civil Liberties in Nigeria: A Political Evaluation of the Digital Rights and Freedoms Bill. *Journal of Current Research and Studies*, 3(4), 1-19.

*COPYRIGHT

© 2026 Olamide Emmanuel ABE.

This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC BY\)](#). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms

Cybersecurity and Civil Liberties in Nigeria: A Political Evaluation of the Digital Rights and Freedoms Bill

Olamide Emmanuel ABE¹, Hameedat Boluwatife ADEAGBO², Aondona, Precious Msendoo³ & AWOSEJO Oluwagbohunmi Abigeal⁴

^{1,2,3,4}Department of Political Science University of Ibadan, Oyo State, Nigeria

Abstract

The global system current is defined by rapid digital transformation, the intersection between cybersecurity and civil liberties, which is the focal point of national and global political discourse. As Nigeria, a country in the Global South, expands into the digital economy, balancing its national security with the protection of fundamental rights is complex. The Digital Rights and Freedoms Bill (DRFB) is a legislative initiative aimed at protecting the rights of citizens within Nigeria's digital ecosystem. So, the study examines the DRFB, a legislative response to the growing threats to online privacy, freedom of expression, anonymity, and the right to digital participation, where surveillance, data breaches, internet shutdowns, and repressive cyber laws have raised democratic concerns. The DRFB is expected to redefine the digital governance within the Nigeria system. The central objective of this study is to politically evaluate the Digital Rights and Freedoms Bill to uphold cybersecurity and safeguard civil liberties in Nigeria. Using qualitative, thematic content analysis of the core provisions of the DRFB, which was supported by an interpretivist framework to contextualise the Bill within Nigeria's political and legal systems. Academic literature, legal documents, and policy frameworks for robust analysis within the system. Findings reveal that while the DRFB introduces protections for the civil liberties of the citizenry and the government for governance purposes in areas such as digital privacy, freedom of information, e-governance, and ICT development, it faces challenges in legal harmonisation, institutional readiness, and political will from the political class in the country. Moreover, there is a lack of clarity in reconciling the bill with contradictory legislation within the country. The DRFB is a transformative bill within the Nigerian socio-political system; however, it requires refinement, robust implementation mechanisms, and cross-sectoral collaboration to actualise its promises within the socio-political system of Nigeria.

Keywords:

Cybersecurity, Civil Liberties, Digital Rights, Legislative Evaluation, E-Governance.

1.0 Introduction

The World has moved into a new epoch, called the digital age. In this epoch of human civilisation, the protection of civil liberties in cyberspace is a defining issue for democratic governance in the Global South, such as Nigeria. The proliferation of digital technologies and increased reliance on the internet for communication and other forms of political engagement raised questions about the limits of state power and how to safeguard individual freedoms within the state. At all levels of governance, governments' adoption of cybersecurity laws serves as a response to rising threats posed by cyber terrorists through disinformation. Also, within states, there are concerns about the abuse of power that have grown increasingly salient in the Global South. The tension between national security and protecting citizens' digital rights demands legislative attention. The Digital Rights and Freedoms Bill represent an attempt to codify the principles of digital freedom in Nigeria's legal architecture. However, its stagnation in the legislative process is due to political and institutional contradictions.

The Digital Rights and Freedoms Bill were introduced in the year 2016 to address the legal vacuum around digital rights and safeguard human online expression and internet governance in Nigeria (Adegoke, 2020). It draws from global instruments such as the African Declaration on Internet Rights and Freedoms (2014) and the Universal Declaration of Human Rights (1948) to domesticate these principles in Nigeria's legal framework. Among the major provisions are protections for freedom of expression online, safeguards against unlawful surveillance, and mandates for transparent data processing by public and private entities. In Nigeria's socio-political system, the bills can be seen as a bill with a progressive orientation due to the political economy of the country, but it was vetoed by the immediate administration of President Muhammadu Buhari in 2019, citing overlaps with existing laws and potential regulatory ambiguities. Several reports documented how some existing laws, such as the Cybercrimes (Prohibition, Prevention, etc) Act of 2015, were enforced to target journalists, critics, and civil society activists (CIPESA, 2021, cited in Roberts, 2021). In effect, cybersecurity is weaponised by state actors to suppress dissent under the guise of national security. This inhuman trend aligns with what Christou (2020) describes as the "securitisation of cyberspace," where state interests override civil protections. This is due to the absence of a legal framework for digital rights in the country, which leaves many of the citizenry vulnerable to arbitrary violations of privacy. Politically, the failure to pass the bill is a form of systemic weakness in Nigeria's legislative and executive engagement with civil society. Despite wide-ranging consultations with digital rights organisations, technologists, and international partners within and outside the country, the bill's rejection is a form of limited responsiveness of political elites to democratic accountability. As Fadugba (2023) argues, policymaking in the Global South suffers a disconnect between public interest and elite priorities that used to occur in the form of regulations. Furthermore, Nigeria's ambiguous stance on internet regulation engendered a political climate ruled by fear and uncertainty. This is exemplified by the 2021 ban on X (formerly Twitter), which violated domestic laws and international human rights standards (Odole, 2023). Consequently, this study seeks to evaluate the Digital Rights and Freedoms Bill through a political view, which focuses on its implications for cybersecurity governance, civil liberties, and democratic accountability in Nigeria. This study, therefore, examines the bill's provisions, the political and legal shortcomings of its enactment, and its potential to counterbalance state overreach.

2.0 Literature Review

The intersection of cybersecurity and civil liberties is a form of socio-political interaction between the state and the citizens that has become a defining concern as digital technologies permeate every facet of human interaction. In Nigeria, the proliferation of internet usage, the digitisation of public and private services, and the growing reliance on social media for civic engagement exposed gaps in the legal protection of digital rights. Against this backdrop, the Digital Rights and Freedoms Bill is a legislative response that aims was/is to safeguard online freedoms, promote transparency in digital governance, and align Nigeria's legal framework with international human rights standards. However, despite its innovative provisions from civil society organisations, the bill's stagnation is a representation of political and institutional challenges. This section reviews relevant literature on the global and regional imperatives for digital rights legislation, the socio-political impact of cybersecurity in Nigeria, and the implications of digital governance on democratic consolidation for the country.

2.1 Cybersecurity

Cybersecurity refers to the collective measures, technologies, and processes designed to protect digital systems, networks, and data from unauthorised access, attacks, or damage (through the activities of a Hacker). With the expansion of digital infrastructure, the cyber system and cybersecurity are national and global security priorities (Singer & Friedman, 2013). The concept is a technical safeguard, and it is also about institutional policies that aim to preserve the confidentiality, integrity, and availability of information (Pfleege & Pfleege, 2012). In today's interconnected world, cyber threats are from state and non-state actors that range from cybercriminals to politically motivated hackers. Cybersecurity threats are diverse and evolving within the digital space. They are malware, phishing, denial-of-service attacks, ransomware, and advanced persistent threats (APT), all of which cripple infrastructure or compromise sensitive data (Chertoff & Simon, 2017). In Nigeria, the limited digital literacy and weak regulatory environments make cybersecurity a pressing challenge (Okeji et al., 2024). The Nigerian Communications Commission (NCC) and the Office of the National Security Adviser (ONSA) have implemented various strategies to mitigate cyber risks in the form of the National Cybersecurity Policy and Strategy (NCPS) of 2021.

2.2 Governance

Governance refers to the mechanisms, processes, and institutions through which authority is exercised and decisions are made, implemented, and monitored in a society. It is beyond the government to include other non-state actors such as civil society, the private sector, and international organisations (Rhodes, 1996). Governance includes various dimensions: political, economic, and administrative management of public affairs (Weiss, 2000). Good governance, as promoted by international bodies such as the United Nations Development Programme (UNDP), talks about principles such as transparency, accountability, the rule of law, participation, and responsiveness (UNDP, 1997). In democratic societies, governance is to ensure that power is exercised responsibly and that citizens are actively involved in public decision-making to bring about development within the system. Historically, the conceptual development of governance is from the critique of state-centric models of public administration that failed to address the complexity of contemporary political systems. As states became more interdependent as globalisation deepened within the

international system, many consider that diverse actors in decision-making emerged (Kooiman, 2003). This led to the articulation of governance as a multi-actor, multi-level process involving negotiation, coordination, and regulation among stakeholders. In the African context, weak governance structures have been identified as major impediments to development, leading to inefficiency, corruption, and poor public service delivery (Hyden, 2012). The structure of governance varies across political systems and is classified into vertical and horizontal dimensions. Vertical governance relates to hierarchies of authority from the national to local levels, while horizontal governance addresses coordination among different branches of government and between public and private actors (Pierre & Peters, 2000).

2.3 Civil Liberties

Civil liberties are the fundamental rights and freedoms that protect individuals from excessive governmental control, that equally ensure the ability to exercise autonomy and participate freely in public life. Rooted in liberal democratic philosophy, civil liberties are a freedom of expression, association, religion, privacy, and the right to a fair trial (Barendt, 2005). These liberties are enshrined in national constitutions and international legal instruments such as the Universal Declaration of Human Rights (UDHR, 1948) and the International Covenant on Civil and Political Rights (ICCPR, 1966). In Nigeria, civil liberties are guaranteed by Chapter IV of the 1999 Constitution (Federal Republic of Nigeria, 1999). The inclusion of these liberties in foundational legal frameworks signifies their role as pillars of democracy, and it does not limit state power but also empowers citizens to engage in political, social, and cultural life without fear of the state. From a historical view, the evolution of civil liberties is shaped against authoritarianism, colonialism, and various forms of discrimination that took place in different eras in state administrations. The Enlightenment era and the rise of constitutional democracies in the 18th century brought civil liberties to the forefront of political discourse (Heywood, 2015). In Nigeria, colonial rule restricted freedoms, but the post-independence epoch saw the formal adoption of civil rights principles. However, military regimes (1966–1999) affected these liberties, which caused a widespread suppression of dissent, arbitrary detention, and media censorship (Osaghae, 1998). The return to democracy in 1999 marked a new era. Whereas, in contemporary society, civil liberties are challenged through technological advancements and digital governance within the system, such as surveillance and algorithmic profiling that present new threats to freedom of expression globally (Zuboff, 2023).

2.4 Global Perspectives on Cybersecurity

The global discourse on cybersecurity is an interplay between state interests, the private sector, and civil society concerns to protect the users of the internet. As Deibert (2013) argues, the internet evolved into a contested space where transnational corporations increasingly dictate access to information, prioritising profit over digital rights. This study states the erosion of network neutrality and the outsourcing of cyberspace regulation to private actors, a trend known as “intermediary liability.” In this framework, private corporations are coerced or incentivised to monitor and restrict online activities under the guise of cybersecurity, raising critical questions about the legitimacy and accountability of such arrangements. Czuryk (2022) posits its argument on the legal and constitutional dimensions of cybersecurity on how it justifies restrictions on human and civil rights, and states that within the global system cybersecurity is invoked as a rationale for limiting freedoms; such measures are proportionate, exceptional, and anchored on national security considerations of the state. This introduces a legal paradox: in protecting the state from

cyber threats, governments (state actors) themselves become sources of rights violations, and draws attention to the growing trend of declaring states of emergency in response to cyber threats, where fundamental rights are curtailed in the state. Shackelford (2021) explores this paradigm that access to secure and open internet infrastructure is fundamental to the exercise of freedoms such as speech, expression, and information sharing within the system. Drawing from the theory of polycentric governance and the principles of corporate social responsibility (CSR), the study advocates a multistakeholder approach to “cyber peace.” This model promotes a state-led effort and also the involvement of civil society, academia, and the private sector in the protection of cyberspace. In terms of global development, Hohmann, Pirang, and Benner (2017) examine the uneven capacity of states to address cybersecurity challenges. The study identifies a vulnerability among developing nations that are rapidly digitising without corresponding investments in cyber infrastructure, which is a potential for cyberattacks to paralyse national networks, as exemplified by the denial-of-service attack in Liberia. According to this study, cybersecurity is not a technical concern but a foundational element for achieving sustainable digital economies. International institutions such as the World Bank and ITU thus elevated cybersecurity in their development agendas, is a form of recognising that trust in digital systems is a prerequisite for inclusive growth and innovation. Finally, Calderaro and Craig (2020) examined the global inequalities in cybersecurity governance and capacity building. The study argues that cybersecurity policies are shaped by the geopolitical and economic dominance of Global North actors, sidelining the needs and voices of countries in the Global South. This imbalance perpetuates dependency and marginalisation as international cooperation tends to be framed in ways that show the Northern interests and priorities.

2.5 The State of Cybersecurity in Nigeria

In the contemporary digital epoch of civilisation across states, the importance of cybersecurity as a national imperative has become more pronounced, given the alarming surge in cyber threats targeting individual users and governmental institutions. This section of the literature review systematically presents the nature of cybersecurity challenges in Nigeria, from its legal, institutional, socioeconomic, and ethical dimensions, to provide a panoramic view of the vulnerabilities and the avenues for reform. Alabi (2024) looks into the foundational perspective of cybersecurity in Nigeria and argues that Nigeria's cybersecurity architecture is affected by infrastructural deficiencies, low public awareness, and weak enforcement of existing legal frameworks, using the Cybercrime Act of 2015 as a case study. This study identifies a pressing need for a holistic and integrated cybersecurity strategy that addresses the technological gaps and systemic policy failures in the country. So, in the country, the pervasiveness of cybercrime ranges from financial fraud to identity theft, which severely affects the country's digital trust and economic stability. Also, from the sociological aspect of cybercrime, Idowu and Madaki (2021) examine the demographic patterns of cybercriminals and find that youth unemployment, socio-economic dislocation, and the allure of illicit wealth are primary drivers for the youth's involvement in cybercrime within the Nigerian political system. On the policy and institutional front, Falode (2021) asserts that cybersecurity transcends technical security; it is integral to national security and economic development within the political system of the Nigerian state. The study uses a comprehensive account of Nigeria's proactive steps, such as the establishment of specialised cybersecurity agencies and compliance with global standards such as the EU's GDPR. Falode states that as Nigeria was reliant on cyberspace for socio-economic and political

activities, its cyber defense systems must evolve to safeguard national sovereignty and economic interests of the state and its citizenry, who are state citizens and aliens that are within the political system.

Furthermore, Uzoka et al. (2025) study balances the nature between cybersecurity, privacy, and civil liberties in the Nigerian political system, expanding on the state's digital governance. Through enabling laws and comparative international conventions within the Nigerian state, the authors articulate how the aggressive digitisation of services and surveillance mechanisms could erode constitutionally guaranteed rights if left unchecked in the Nigerian political system. Furthermore, some legal frameworks are available in some countries that uphold civil liberties to combat cyber threats, also, many of these countries within the global system navigate toward advanced technological domains in the form of artificial intelligence. Nte, Enoke & Teru, (2022) study contributes a comparative dimension to the discourse by analysing Nigeria's cybersecurity legal system alongside that of South Africa. Also, nations within the Northern hemisphere face similar cybercrime that is not different from the Global South. However, some in the Global North made progress in legal harmonisation as well as in public-private partnerships; by contrast, some in the Global South continue to face fragmented policies, while the state of cybersecurity in Nigeria is precarious, as evidenced by persistent structural weaknesses and the rapid evolution of cyber threats.

2.6 Cybersecurity in Africa

The African continent, though progressively integrating into the global digital economy, is challenged by cybersecurity problems as it confronts others within the global system. Various studies within the African scientific community look into how African nations face the dynamics of cybersecurity in terms of policy and societal trust. Osunji (2022) conducted a qualitative study to examine the role of government in the advancement of cybersecurity building capacity efforts in Uganda through the implementation of the Cybersecurity Capacity Maturity Model for Nations (CMM) and it was revealed that there is a nexus between governmental action and the public's trust in digital infrastructures in the state. Also, the failure to finalise and implement a national cybersecurity strategy resulted in an ad hoc a fragmented response to digital threats in Uganda's political system. Furthermore, the absence of political prioritisation and low awareness among policymakers hampers the visibility and impact of cybersecurity initiatives in the country, and some of these systemic weaknesses erode public confidence in online platforms and services within the country, which is common to countries in the Global South hemisphere. Kwabena-Adade and Yeboah-Boateng (2022) examine the implications of 5G deployment on cybersecurity in Ghana. Although in Ghana, the 5G technology promises substantial improvements in data speed, bandwidth, and latency. In another instance, the proliferation of IoT and smart infrastructure introduce new cybersecurity treat to the community of human, through the decentralisation of data on edge computing and the increased exposure to machine-to-machine communications heighten the risk of data breaches and cyberattacks. The study identifies regulatory gaps, lack of compliance standards, and weak enforcement mechanisms as principal challenges in Ghana's cybersecurity system, as is common in many Third World Countries.

Sawaneh, Kamara, & Kamara (2021) from a sociocultural analysis of cybersecurity challenges in Sierra Leone note that the proliferation of mobile technology and internet access has democratised information dissemination, transforming every citizen into a potential content creator. While this digital participation promotes freedom of expression, it also

facilitates cybercrimes such as online fraud, misinformation, and digital propaganda. The COVID-19 pandemic intensified these trends, illustrating the volatility of digital spaces during periods of national crisis, and situates cybersecurity as a technical or policy concern and as a social phenomenon that requires a behavioural change and educational interventions in a state. Sutherland (2017) accounts for the cybersecurity governance in South Africa, identifying the National Cybersecurity Policy Framework (NCPF) and the Protection of Personal Information Act (POPIA) as foundational instruments in securing cyberspace. South Africa's approach is a more advanced institutional framework compared to other African countries, with state agencies responsible for data privacy enforcement and cybersecurity implementation. Nevertheless, the study critiques the centralisation of cybersecurity leadership under the Ministry of State Security, raising concerns about transparency, civil liberties, and the balance between national security and citizen privacy.

Table 1: Summary of Reviewed Studies

Author(s)	Year	Study Purpose	Methodology	Key Findings	Policy Implications
Osunji	2022	Examine the government's role in cybersecurity capacity building	Qualitative case study, interviews; thematic analysis using ATLAS.	Lack of national strategy, poor funding, and political apathy weaken cybersecurity capacity	For the immediate ratification of the national cybersecurity strategy and digital education investment
Kwabena-Adade & Yeboah-Boateng	2022	Explore cybersecurity risks with 5G deployment	Conceptual review	5G introduces IoT vulnerabilities and lacks regulatory oversight	Call for regulatory standards and cybersecurity compliance frameworks
Sawaneh, Kamara & Kamara	2021	Discuss cybercrime in the social media age	Descriptive study	Digital platforms are exploited for fraud, misinformation, and propaganda	Strengthen digital literacy and develop content moderation policies
Sutherland	2017	Investigate institutional cybersecurity governance	Policy analysis	POPIA and NCPF offer a legal structure, but centralisation limits public trust	Multi-stakeholder frameworks that promote transparency and efficiency for monitoring cybersecurity.
Alabi	2024	To assess cybercrime threats and evaluate the effectiveness of Nigeria's cybersecurity framework	Literature review using primary and secondary sources	Inadequate infrastructure, weak enforcement of the Cybercrime Act 2015, and low awareness fuel cybercrime	Improve infrastructure, awareness campaigns, and enforcement of laws
Idowu & Madaki	2021	To examine the challenges of	Survey of 150 respondents in Abuja	Cybercrime is largely driven by unemployed	Create jobs, sensitise the public,

		cybercrime control in Nigeria		youths (21–35), poor legislation, and societal decay	enact/enforce stronger cyber laws
Falode	2021	To analyse Nigeria's cybersecurity policy as a tool for national security	Policy analysis within the global system	Nigeria has agencies and laws in place; compliance with global standards like GDPR is progressing	Capacity-building and harmonisation with global frameworks
Uzoka, Umejiaku & Onyekachukwu	2025	To analyse the balance between privacy, security, and civil liberties in Nigeria's digital era	Legal and policy review; comparative and analytical approach	Technological advancement increases intrusion into personal data; legal protections are insufficient	To develop a legal framework to ensure transparency, regulate surveillance, and protect civil liberties
Nte, Enoke & Teru	2022	To compare cybersecurity laws and policy frameworks between Nigeria and South Africa	Comparative legal analysis	Nigeria's cybersecurity policy is fragmented and reactive; South Africa demonstrates stronger implementation mechanisms	Harmonise national frameworks and strengthen regulatory enforcement through cross-national collaboration
Azubuike	2023	Analyses the motivations and impacts of state-sponsored cyberattacks in the context of international conflicts and global security.	Secondary data collection, content, and historical analysis, securitisation theory	Cyberattacks are driven by economic, political, and national security interests. Technological capabilities enable these attacks. Cyber threats are politically constructed.	Using a combination of preventive and responsive strategies, such as diplomatic, legal, and technical measures.
Deibert	2011	The role of civil society, intermediary liability, and private sector responsibilities in global cyberspace governance	Analytical commentary with examples from Canada and OECD meetings	Private sector entities are increasingly involved in state-driven surveillance and control, often without judicial oversight. Market priorities frequently undermine	Advocates for transparency, judicial accountability, and civil society engagement in shaping internet governance. Warns against the unchecked delegation of policing roles to intermediaries.

				privacy and neutrality.	
Czuryk	2022	Legal basis for restricting human rights in the name of cybersecurity	Legal-analytical approach	Cybersecurity, though not explicitly named, underpins state security justifications for limiting civil liberties during emergencies.	Calls for clearer legal definitions and proportional frameworks to balance individual freedoms and national security in cyberspace.
Shackelford	2021	Conceptualising cybersecurity as a human right and promoting cyber peace	Interdisciplinary analysis using legal theory, CSR, and humanities	Recognising cybersecurity as a human right to strengthen global cyber peace and institutional responsibility. CSR and polycentric governance are crucial to this evolution.	Call for an interdisciplinary and global approach to cybersecurity governance (such as workforce development, education, and ethical frameworks).
Hohmann, Pirang, & Benner	2017	Cybersecurity capacity building and resilience in developing countries	Policy research and case analysis	Developing countries face disproportionate cybersecurity risks due to weak ICT infrastructure. Cyberattacks destabilise entire nations.	Prioritising cybersecurity in global development. Recommends international cooperation, investment in ICT security, and strategic alignment with economic growth.
Calderaro & Craig	2020	Transnational governance and inequalities in cybersecurity capabilities	Comparative policy study	Global disparities in cyber capacity show a systemic inequality. Wealthier nations dominate governance frameworks, sidelining the global South.	Advocates for inclusive, equitable cyber governance that calls for capacity building in low- and middle-income countries within the Global South through fairer international partnerships.
Margulies	2017	Examines U.S. cybersecurity, surveillance, and privacy policy under the Obama administration post-Snowden disclosures.	Legal and policy analysis of U.S. federal actions	Post-Snowden, the Obama administration employed soft law (non-binding policies, agreements) and agency discretion	There is a need for a balanced approach combining transparency, stakeholder engagement, and enforceable norms.

				(federal agency actions). Also, developed a US-EU Privacy Shield to address transatlantic data transfer concerns.	
--	--	--	--	---	--

Source: Authors Compiled

3.0 Methodology

This study adopts a qualitative research design to evaluate the intersection of cybersecurity governance and civil liberties in Nigeria, focusing on the political dimensions that surround the Digital Rights and Freedoms Bill (DRFB) within Nigeria's political system. Therefore, the choice of a qualitative methodology is informed by the nature of the research questions, which aim to explore policy discourses, institutional practices, as well as the normative implications of digital governance frameworks (Creswell & Poth, 2016). This allows for an exploration of factors that shape the formulation and implementation of cybersecurity legislation as they relate to fundamental civil rights within the Nigerian political system.

Data for the study are drawn from secondary sources. These are legislative instruments such as the Cybercrimes (Prohibition, Prevention, etc.). Act 2015, which is the National Cybersecurity Policy and Strategy (NCPS), official communications from NCC and NITDA, judicial opinions, policy briefs, and peer-reviewed academic literature. While the Digital Rights and Freedoms Bill serve as the central unit of analysis, there are other supporting documents used to trace its political trajectory and operational gaps. The study employs content analysis as its principal method of data analysis. This involves the use of a systematic coding and thematic evaluation of documentary to identify patterns, contradictions, and normative orientations in Nigeria's cybersecurity governance. Deductive coding strategy aligned with constructs of transparency, accountability, digital rights protection, and political oversight to interrogate the alignment between existing cybersecurity policies and international standards, such as those set by the African Declaration on Internet Rights and Freedoms and the UN's Guidelines on Digital Rights (Kulesza & Balleste, 2015). Special attention is given to tracing the ethical and political tensions inherent in cybersecurity practices, those that implicate freedom of expression, privacy, and access to information. Finally, the study incorporates an ethical dimension by engaging with the normative discourse on cybersecurity and civil liberties. Drawing on the exploration of ethics in digital innovation to examine how cultural and institutional values interact to shape public perceptions on cybersecurity and civil rights within the Nigerian political domain enables the development of a cultural framework that integrates ethical accountability into digital governance.

3.1 Theoretical Framework

Governance Theory is a late 20th-century response to the limitations of traditional state-centric models of public administration. It came into the light with growing recognition that the state was no longer the sole actor in the

formulation and implementation of public policy in a state or within the global system. So, from the micro level, governance is a product of interactions among diverse actors within a political system, which can be state actors, civil society, market forces, and international organisations (Rhodes, 1996; Pierre & Peters, 2000). It also gained prominence in the wake of neoliberal reforms and globalisation, which eroded the capacity of centralised states to govern in interdependent societies. Within political science and public policy, governance came to denote government action and processes through which societies are steered through rules, networks, norms, and institutions (Kooiman, 2003).

Governance Theory is built on several foundational assumptions that help in the formation of the central theme of this study. It assumes a pluralistic policy environment, where multiple actors, such as state agencies, non-governmental organisations, private sector actors, and transnational bodies, interact in the policy process (Stoker, 1998). Second, it posits that governance is characterised by networks rather than hierarchies and is based on horizontal coordination, negotiation, and mutual adjustment over top-down command-and-control mechanisms (Rhodes, 1997). Also, governance theorists are assumed to function when embedded in frameworks of transparency, accountability, and stakeholder participation in a system (Bevir, 2012). One of the primary critiques is its conceptual ambiguity. Scholars argue that “governance” is used in an overly broad and imprecise manner, making it difficult to distinguish from traditional forms of administration (Jessop, 1998). Furthermore, critics note that networks and partnerships obscure power asymmetries in a system and that this allows powerful actors to dominate under the guise of consensus (Davies, 2011).

Governance Theory is a robust analytical framework for evaluating political and institutional dimensions of cybersecurity and civil liberties in Nigeria's political system, as this facilitates how state and non-state actors interact in the development and implementation of digital policies such as the Digital Rights and Freedoms Bill (DRFB), within the governance paradigm. Furthermore, Governance Theory supports the analysis of institutional fragmentation and coordination challenges within Nigeria's digital regulatory architecture, such as the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), and security operatives. Thus, Governance Theory explains existing policy dynamics and also offers prescriptions for building a more accountable, rights-respecting digital governance regime in Nigeria.

3.2 Findings and Discussion

Table 2: Qualitative Analysis of the Digital Rights and Freedoms Bill

Thematic Area	Provision Focus	Key Implications	Primary Beneficiaries	Identified Gaps/Challenges	Recommended Policy Direction
Online Privacy and Data Security	Legal recognition of digital privacy; mechanisms for data disclosure	Improve the digital security, enforce lawful surveillance boundaries, and build public trust	Citizens, journalists, data subjects, human rights defenders	Conflicting laws (MACMA 2016), weak enforcement, and low public awareness	Legal harmonisation, establishment of a data protection authority, and public digital rights literacy campaigns
Anonymity	Right to access the internet	Strengthens civil liberties,	Whistleblowers, activists,	Criminalisation under the	Revisit anonymity clauses in extant

	without identity and protection for vulnerable actors	protects dissidents, and limits state surveillance	journalists, and minority	Cybercrimes Act, identity verification mandates, and misuse	laws, legal clarity on permitted anonymous activities, and secure tools for ethical anonymity
Freedom of Expression Online	Guarantees free digital speech; prohibits content takedown without judicial sanction	Protection against censorship, improving digital civic participation, and legal checks	General public, civil society, online creators	Ambiguities in the Cybercrimes Act, state-sponsored disruptions, and weak judicial enforcement	Repeal vague legal clauses, codify content takedown procedures, and penalise arbitrary internet disruptions
Right to Internet Access and Freedom of Information	Recognises the internet as a right for fair broadband access and content freedom	Bridges digital inequality, promotes informed citizenry, and empowers rural communities	Rural dwellers, students, low-income earners, and digital entrepreneurs	Poor connectivity in rural areas, affordability issues, and regulatory delays	Treat broadband as a utility, incentivise infrastructure in rural zones, and enforce equitable spectrum allocation
Digital Expression and Online Assembly	Legalises digital gathering, advocacy, and expression through online platforms	Expands civic engagement tools, validates digital protests, and strengthens participatory governance	Civil society organisations, youth groups, and advocacy networks	State surveillance, regulatory overreach, and platform monopolies	Legal safeguards for digital assembly, localised alternatives to dominant platforms, and regulatory checks on big tech
Right to Create Public Knowledge and Promote ICT Skills	Promotes digital literacy, ICT integration in education, and access to open learning resources	Develops human capital, boosts educational innovation, and empowers the workforce	Students, educators, researchers, lifelong learners	Poor funding for ICT in schools, certification legitimacy issues, and teacher skill gaps	Standardise digital credentials, invest in teacher ICT training, and support public digital content repositories
E-Governance and Financial Transparency	Encourages digital public service delivery, national ID integration, and open government platforms	Fosters institutional efficiency, curbs corruption, and promotes citizen engagement	General public, government agencies, service providers	Institutional resistance to digital reform, ID fraud risks, and fragmented implementation	Enforce digital governance compliance, strengthen NIMC frameworks, and integrate feedback systems for e-citizenship

4.0 Discussion

4.1 Online Privacy and Data Security

The Digital Rights and Freedoms Bill (DRFB) are a progressive legislative intervention aimed at protecting the rights of Nigerian citizens in the digital space, with emphasis on the right to online privacy. Although the Nigerian Constitution guarantees the right to privacy under Section 37, this right has not been extended explicitly to other forms of online activities, which are central to daily life in the present political dispensation. The DRFB addresses this lacuna by recognising digital privacy as a distinct and legally protectable right for the state citizens. This recognition is given due to the increasing reports of data breaches among the citizens, unauthorised surveillance, and the commercialisation of personal data without consent within the political system. Also, the Bill introduces mechanisms such as mandatory court warrants for data disclosures on an individual or corporate organisation, notifications, as well as publication of government requests for user data, which is an international best practice, and transparency about digital information. One strength of the DRFB is its regulation of surveillance, which is the interception of digital communications within the system. The Bill further introduces procedural safeguards that prevent arbitrary interference by security agencies, that allow only judicial oversight for data access, and mandates post-disclosure warrants in exigent situations.

4.2 Anonymity

In the discourse on digital rights in Nigeria, the principle of anonymity stands as a cornerstone in safeguarding civil liberties in a political environment where state surveillance and political repression are on the rise. The Digital Rights and Freedoms Bill (DRFB) introduce a commendable provision that permits individuals to access the internet without disclosing their identities. This affirms the right to anonymity as a mechanism for self-protection for people under the categories of journalists, whistleblowers, human rights defenders, and other vulnerable groups operating within a volatile socio-political system of Nigeria. The anonymity clause gives individuals the opportunity to use technical safeguards that obscure their identity, which limits the unauthorised collection and use of personal data. In doing so, it reinforces the objectives of privacy, freedom of expression, and the preservation of personal dignity in digital spaces. The internet, as a decentralised platform for democratic engagement, has thus become a refuge and a battleground for expression. The Cybercrimes (Prohibition, Prevention, Etc.) The Act of 2015 criminalises the use of technologies intended to obscure identity with criminal intent. Though this seems aligned with public interest objectives, the broad and ambiguous language employed in the Act may facilitate overreach and arbitrary interpretation. Similarly, regulations such as the Registration of Telephone Subscribers Regulations and the Framework for Public Internet Access require identity verification, thus undermining the essence of anonymous digital engagement.

4.3 Freedom of expression online

The Digital Rights and Freedoms Bill (DRFB) is a paradigmatic shift in the architecture of digital governance in Nigeria. With its explicit emphasis on safeguarding freedom of expression in the online domain, the Bill serves as a normative

framework that seeks to align Nigeria's legal instruments with democratic principles and international human rights standards. Rooted in Section 39 of the 1999 Constitution of the Federal Republic of Nigeria (as amended), the DRFB extends the constitutional guarantee of free expression into the digital sphere, a transformative role of digital technologies in contemporary civic life. Furthermore, the Bill mandates that any attempt by state or non-state actors to restrict access to digital content must be sanctioned by a court of competent jurisdiction. This legal threshold affirms the rule of law and is designed to avert arbitrary content takedowns and state-sponsored information control. Provisions prohibiting practices such as internet throttling, signal jamming, and shutdowns demonstrate the Bill's intention to preserve the infrastructural integrity of the digital public sphere. These safeguards are in place due to the former state actions such as the disruption of internet services during the #EndSARS protests. One of the Bill's most commendable features is its deliberate effort to harmonise Nigeria's digital rights with regional and international human rights instruments. This intent becomes salient when contrasted with existing laws, such as the Cybercrimes Act (2015) Section 24(b), which criminalises electronic communications deemed annoying or inconvenient.

4.4 Right to Internet Access and Freedom of Information

A fundamental pillar of the DRFB is the legal recognition of internet access as a right, reinforcing the idea that individuals, irrespective of geographical or economic constraints, from able to connect to the digital world. This right extends to underserved populations in rural and low-income urban areas, where affordability and connectivity are persistent barriers. The Bill explicitly grants individuals the liberty to seek and consume information online, placing necessary limitations on content that poses direct threats to societal harmony and individual safety (such as child sexual abuse material, hate speech, defamation, incitement to violence, and genocidal propaganda). The Bill reinforces broadband as a public utility that must be equitably distributed for socio-economic imperatives of digital inclusion. The Bill codifies the right to express oneself online and prohibits unwarranted censorship or denial of internet access. Citizens are entitled to receive information and also to share opinions, engage in commercial activities, and participate in public discourse without unjust interference.

4.5 Digital Expression and Online Assembly

A cornerstone of democratic engagement is the right to peaceful assembly and association, traditionally exercised in physical spaces. The DRFB recognises the evolution of civic interaction by affirming this right within the digital environment. It extends constitutional protections to those enshrined in Section 40 of the 1999 Constitution of the Federal Republic of Nigeria (as amended), to the digital realm that permits individuals and groups to congregate, deliberate, and advocate through any online platforms as available within the Nigerian political system. In an era of digital capitalism, the DRFB anticipates the risks associated with market monopolisation within the information and communication technology (ICT) ecosystem. This provision finds resonance in the Federal Competition and Consumer Protection Act, which mandates oversight over anti-competitive behaviour. Notably, the powers extend to domestic and international entities operating within Nigerian digital markets. However, there is a lack of clarity on the

jurisdictional overlaps between the Federal Competition and Consumer Protection Commission (FCCPC) and potentially the National Human Rights Commission (NHRC) that warrants legislative refinement. Digital

4.6 Literacy as a Fundamental Right

One of the most transformative aspects of the DRFB is its recognition of learning as a foundational digital right. In moving beyond abstract ideals, the Bill mandates the integration of internet literacy, media awareness, and digital security modules into formal school curricula. This is a policy shift in Nigeria that foregrounds knowledge as the first line of defense in the digital age within the global system. Also, the bill, unlike the aspirational provision of free education in Chapter Two of Nigeria's 1999 Constitution largely symbolic due to its non-justiciable nature in the country, the Bill proposes grounded and pragmatic strategies for affordable and accessible digital education for all. Also, the Bill extends this right to persons with disabilities, aligning itself with international conventions such as the UN Convention on the Rights of Persons with Disabilities. A forward-looking component of the Bill is its directive to educate learners about the dangers embedded within digital environments. In terms of the modules on managing online harm, information disorder (such as misinformation and disinformation), and safeguarding personal privacy. In a heterogeneous society such as Nigeria, the hegemony of languages in digital education will exacerbate marginalisation. The Bill disrupts this trajectory by mandating that learning resources be made available in diverse linguistic forms, so that no ethnic or linguistic community is systemically excluded from the digital knowledge economy.

4.7 Safeguarding Learners' Privacy in a Digitally Converged Educational System

Also, the DRFB is a robust framework for safeguarding the privacy of students and learners, positioning it as a statutory obligation and as a fundamental right within the digital and physical learning spaces. This reconceptualisation of privacy as *inalienable* aligns seamlessly with Section 37 of Nigeria's Constitution, which guarantees the right to personal privacy, as well as with the Nigerian Data Protection Regulation (NDPR). In the educational system that is available within the Nigerian state, the Bill recognises the intensifying risks associated with student data misuse. From surveillance tools used in the Learning Management Systems (LMS) for the harvesting of metadata via online learning platforms, students are exposed to threats they are neither equipped to resist nor able to. From this bill, there is a shift in the paradigm from opaque institutional data practices to one grounded in transparency and accountability. The Bill also makes a progressive declaration by recognising the intellectual property rights of students over their digital creations. The Bill critiques the conflation of privacy policies with contractual obligations requiring consent as a misinterpretation of the NDPR.

4.8 The Right to Create Public Knowledge

At the core of this provision is the recognition that *knowledge creation* is no longer the exclusive preserve of traditional academic institutions or research bodies. The DRFB codifies the right of all individuals, irrespective of formal educational status, to acquire and also produce, validate, and disseminate knowledge through the use of digital platforms to develop and share open educational resources (OERs). One of the components of the Bill is its directive

to integrate ICT into teaching and learning. This does not refer to the deployment of technological tools in classrooms but to a pedagogical transformation where technology becomes a medium for collaborative inquiry. The Bill rightly identifies access to knowledge and learning materials as a foundational right. In doing so, it demands that educational content and collaborative tools be made available at an affordable rate.

4.9 E-Governance and Financial Transparency

At the heart of the DRFB's e-governance provision is the aspiration for a digitally enabled, transparent, and participatory model of governance. The Bill calls for the creation of a modernised self-governance architecture that digitises service delivery and promotes reciprocal information exchange between state institutions and citizens. This reimagines governance not as a top-down exercise of authority but as a dynamic dialogue sustained through digital interaction that occurs over time within a socio-political system. It echoes the E-Government Masterplan of Nigeria, a coordinated national strategy that promotes interoperability, decentralisation, and accessibility of public services through technology. The DRFB also urges public institutions to harness the communicative power of social media platforms as instruments of democratic engagement, including Nigeria's Framework and Guidelines for the Use of social media in Public Institutions, which encourages citizen feedback, dissemination of public information, and transparent government-citizen interaction. Furthermore, it mandates the development of a credible national identity infrastructure that leverages digital technologies to reduce fraud, eliminate redundancy, and combat identity theft. Therefore, the DRFB functions as both a legislative mandate and a moral imperative that compels all tiers of government toward digitisation, not as a trend but as a constitutional obligation to transparency, accountability, and service excellence.

5.0 Conclusions

In the global system, there are escalating cybersecurity threats and increasing state surveillance. Nigeria, as a country in the Global South, is not free from this dilemma of balancing the imperatives of national security with preserving fundamental civil liberties in the digital system. However, in the country, the existing legal instruments serve as fragmented protections for the elite, and the absence of a respected digital governance framework gives room for inconsistencies in enforcement, arbitrary data practices, and infringements on freedom of expression, privacy, and access to information within the country's socio-political system. This study sees the Digital Rights and Freedoms Bill (DRFB) as a legislative response to challenges of civil liberties and cybersecurity. So, seven major thematic were analysed: (1) online privacy and data security, (2) anonymity and identity protection, (3) freedom of expression online, (4) internet access and freedom of information, (5) digital expression and online assembly, (6) digital literacy and human capital development, and (7) e-governance and financial transparency. Each theme of the Bill's aspiration is to entrench democratic norms, protect user rights, and promote accountability in Nigeria's digital space. However, contradictions with existing laws, implementation deficiencies, and a lack of interagency coordination affect its transformative potential.

Therefore, the findings about the DRFB, if passed and properly implemented, could serve as a cornerstone for inclusive digital governance in Nigeria. It holds the capacity for civic engagement and socio-economic development that aligns with Nigeria's global policy within the ambit of international human rights standards. Nevertheless, without strategic reforms, the gaps, such as regulatory overlaps, ambiguous cybercrime provisions, and infrastructural inequalities, will continue to affect the public trust and entrench digital marginalisation in the country. This study employed a qualitative approach based on documentary analysis and thematic mapping. However, this methodology provided in-depth information about the bill and cybersecurity in the country, it did not incorporate empirical data through field surveys or interviews with stakeholders in sectors (such as legislators, ICT regulators, or digital rights advocates). Consequently, the findings from this study do not capture the operational challenges experienced by policy implementers in terms of the bill within the Nigerian political system.

So, further studies in this regard should include empirical studies on the lived experiences of Nigerian citizens about their digital rights, comparative studies between Nigeria and other African states with similar legislative systems will also yield valuable lessons for future bills, and evaluation of post-implementation of the DRFB (should it be enacted) to monitor its efficacy and guide periodic legislative review in this regard in the country. Finally, the Digital Rights and Freedoms Bill are more than a legal instrument; it is a defining test of Nigeria's commitment to democratic consolidation in the digital age. As the nation navigates between cybersecurity and civil liberties, bold legislative action, political will, and inclusive policymaking are required so that digital transformation serves the public good, strengthening democracy rather than subverting it.

References

- 1) Adegoke, A. (2020). Digital rights and privacy in Nigeria. *Paradigm Initiative*, 4.
- 2) Alabi, M. (2024). Literature Review on Cybersecurity in Nigeria. *Available at SSRN 4818514*.
- 3) AZUBUIKE, C. F. (2023). Cybersecurity and international conflicts: An analysis of state-sponsored cyberattacks. *Nnamdi Azikiwe Journal of Political Science*, 8(3), 101-114.
- 4) Barendt, E. (2005). *Freedom of Speech* (2nd ed.). Oxford: Oxford University Press.
- 5) Bevir, M. (2012). *Governance: A very short introduction*. OUP Oxford.
- 6) Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917-938.
- 7) Christou, G. (2020). The collective securitisation of cyberspace in the European Union. In *Collective Securitisation and Security Governance in the European Union* (pp. 52-75). Routledge.
- 8) CIPESA. (2021). *The State of Internet Freedom in Nigeria 2021*. Collaboration on International ICT Policy for East and Southern Africa.
- 9) Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications.
- 10) Czuryk, M. (2022). Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues. *Studia Iuridica Lublinensia*, 31(3), 31-43.
- 11) Davies, J. S. (2011). *Challenging governance theory: From networks to hegemony*. Policy Press.
- 12) Deibert, R. (2011). Towards a cybersecurity strategy for global civil society. *Global Information Society Watch*, 2011, 23-26.
- 13) Deibert, R. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal Books.

- 14) Fadugba, A. (2023). *Resistance from Below: Networked Digital Activism in Nigeria* (Doctoral dissertation, State University of New York at Buffalo).
- 15) Falode, A. J. (2021). Cybersecurity policy in Nigeria: A tool for national security and economic prosperity. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 553-563). Routledge.
- 16) Federal Government of Nigeria. (2021). *National Cybersecurity Policy and Strategy*. Abuja: Office of the National Security Adviser.
- 17) Federal Republic of Nigeria. (1999). *Constitution of the Federal Republic of Nigeria*. Abuja: Government of Nigeria.
- 18) Heywood, A. (2015). *Key concepts in politics and international relations*. Bloomsbury Publishing.
- 19) Hohmann, M., Pirang, A., & Benner, T. (2017). Advancing Cybersecurity Capacity Building. *Global Public Policy Institute (GPPI)*.
- 20) Hyden, G. (2012). *African politics in comparative perspective*. Cambridge University Press.
- 21) Idowu, O. A., & Madaki, M. (2021). Cybercrimes and Challenges of Cybersecurity in Nigeria. *International Journal of Sociology and Development*, 3(1).
- 22) Jessop, B. (1998). The rise of governance and the risks of failure: The case of economic development. *International Social Science Journal*, 50(155), 29–45.
- 23) Kooiman, J. (2003). *Governing as Governance*. London: Sage Publications.
- 24) Kulesza, J., & Balleste, R. (Eds.). (2015). *Cybersecurity and human rights in the age of cyberveillance*. Rowman & Littlefield.
- 25) Kwabena-Adade, H., & Yeboah-Boateng, E. O. (2022). Deployment of 5G in Emerging Economies: Cybersecurity Challenges and Potentials for Ghana. In *5G, Cybersecurity and Privacy in Developing Countries* (pp. 107-130). River Publishers.
- 26) Margulies, P. (2017). Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. *Ind. J. Global Legal Stud.*, 24, 459.
- 27) National Assembly of Nigeria. (2018). *Digital Rights and Freedoms Bill*. Lead debate for concurrence from the House of Representatives by Senator Ahmad Lawan (Yobe North – Senate Leader). Federal Republic of Nigeria.
- 28) Nte, N. D., Enoke, B. K., & Teru, V. A. (2022). A comparative analysis of cybersecurity laws and policies in Nigeria and South Africa. *Law Research Review Quarterly*, 8(2), 233-258.
- 29) Odole, E. (2023). *Crisis Communication on X (Formerly Twitter): Information, Misinformation, and the Role of the Federal Ministry of Information and Culture During the EndSars Protest in Nigeria* (Doctoral dissertation, Regent University).
- 30) Okeji, S. M., Adedoyin-Raji, J. O., & Isa, Y. I. (2024). Legal frameworks for the implementation of electronic governance in Nigeria and matters arising. *Environmental Technology and Science Journal*, 15(2), 150-155.
- 31) Osaghae, E. E. (1998). *The crippled giant: Nigeria since independence*. Indiana University Press
- 32) Osunji, O. (2022). *Government's Role in Building Trust and Confidence in the Internet: A Case Study of Uganda in the Implementation of Cybersecurity Capacity Maturity Model for Nations*. Marymount University.
- 33) Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing computer security: A threat/vulnerability/countermeasure approach*. Prentice Hall Professional.
- 34) Pierre, J., & Peters, B. G. (2020). *Governance, politics, and the state*. Bloomsbury Publishing.
- 35) Rhodes, R. A. (1997). Understanding governance: Policy networks, governance, reflexivity and accountability. *Open University*.
- 36) Rhodes, R. A. W. (1996). The new governance: governing without government. *Political studies*, 44(4), 652-667.
- 37) Roberts, T. (2021). Digital rights in closing civic space: lessons from ten African countries. *Institute of Development Studies (IDS)*.
- 38) Sawaneh, I. A., Kamara, F. K., & Kamara, A. (2021). Cybersecurity: A key challenge to the information age in Sierra Leone. *Asian Journal of Interdisciplinary Research*, 4(1), 35-46.

- 39) Shackelford, S. J. (2021). Should cybersecurity be a human right? Exploring the “shared responsibility” of cyber peace. In *Music, Business and Peacebuilding* (pp. 174-197). Routledge.
- 40) Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.
- 41) Stoker, G. (1998). Governance as theory: five propositions. *International social science journal*, 50(155), 17-28.
- 42) Sutherland, E. (2017). Governance of cybersecurity case of South Africa. *The African Journal of Information and Communication*, 20, 83-112.
- 43) UNDP. (1997). *Governance for Sustainable Human Development: A UNDP Policy Document*. New York: United Nations Development Programme.
- 44) United Nations Human Rights Committee. (2004). *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*. CCPR/C/21/Rev.1/Add.13.
- 45) Uzoka, N., Umejiaku, N., & Ijeoma Onyekachukwu, E. O. (2025, March). Using the Instrumentality of Law and Policy in Balancing Privacy Issues, Security, and Civil Liberties in a Digital Era. In *Proceedings of the 19th International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.
- 46) Weiss, T. G. (2000). Governance, Good Governance & Global Governance: conceptual & actual challenges. *Third World Quarterly* 21 (5).
- 47) Zuboff, S. (2023). The age of surveillance capitalism. In *Social Theory Rewired* (pp. 203-213). Routledge.