

Using the Instrumentality of Law and Policy in Balancing Privacy Issues, Security and Civil Liberties in a Digital Era

Ngozi Uzoka¹, Nneka Umejiaku¹ and Eze Onyekachukwu Ijeoma Onyekachukwu²

¹Nnamdi Azikiwe University Awka Anambra state. Nigeria

²Faculty of Law, Nnamdi Azikiwe University Awka, Anambra State Nigeria

nc.uzoka@unizik.edu.ng

no.umejiaku@unizik.edu.ng

eze120@gmail.com

Abstract: Information technology is rapidly changing our world. It avails us with new opportunities to interact, communicate and do businesses. The wide and increased usage of the internet has made communication easy, fast and efficient. On the other hand, information and communication technology also provides an avalanche of avenues through which harm can be perpetrated to our security both individually and collectively. The threats and challenges posed by information technology continue to evolve on daily basis, hence the need to protect our human and constitutionally guaranteed rights. The tug of war between privacy concerns and security has become a defining issue of the digital age. The paper aims to discuss the need for the government to regulate the new threats posed by information technology using the instrumentality of the law. This paper made use of primary sources of data such as such as enabling laws, acts and secondary sources of data, conventions, and journal articles. The study is also analytical and comparative in nature. The paper finds that advanced and sophisticated technology have facilitated constant intrusion into people's personal data and communications. There is need to protect legal, ethical and social values against these constantly up surging technologies. The paper therefore recommends amongst others that there is an urgent need to finding the right equilibrium between privacy threats and constitutionally guaranteed civil liberties as the society embraces emerging technology like artificial intelligence and its likes. Thus, governments need to develop significant legal frameworks to regulate government surveillance steps, increase transparency and implement privacy-enhancing measures.

Keywords: Data protection, Data privacy, Civil liberties, Digital rights, Law, Human rights, Constitutional rights

1. Introduction

The rate and manner at which information technology and digital transformation is taking place is alarming. In the era of digitalization, individuals as well as organizations are increasingly recognizing the need to embrace technology to spontaneously exercise their rights and air their opinions on topical issues. At a time when digital technologies have become an avenue through which people exercise their opinions, thoughts and conversations on issues. Information technology plays a vital role in this modern era, transcending industries and facilitating seamless transfer of information between devices. Digital technology in the form of use of the internet, social media platforms and smart devices has increased economic and cultural changes. These changes bring to the fore complex implications for human rights, civil liberties and data protection and privacy issues that need to be understood. (Sharma G & Bassi A, 2024)

It is without doubt that access to the internet has a wide coverage, even as reliance is being placed on its usage to conduct business effectively, stay connected to friends and family as well as write or comment on public discourse. Hence, the importance of information technology cannot be overemphasized as it enables rapid communication, data transfer, facilitates innovation and competitiveness. The aim of this paper is to analyze the impact of digital technology on human rights in view of the technological advancements. Understanding the implications of human rights in a digital era cannot be over-emphasized. In a digitally connected world, the concept of privacy becomes more complex and intricate as data can be easily obtained, stored and analyzed by various entities that may be countries apart. The avalanche of digital technologies has paved way for unprecedented opportunities for connectivity and progress. On the other hand, it has also opened up channels of data misuse, privacy breaches and cyber threats

The paper also examines how information technological innovations are altering data protection laws, individual's right to privacy and freedom of expression. In an increasingly connected and data driven world, the paper seeks to explore the ethical and legal avenue by which information technological innovations can be checkmated by law. Data protection is the hallmark of preserving individual rights and freedoms in a digital age. Hence, an important element of a lawful state is the presence of guaranteed and protected human rights. The U.S Supreme Court Chief Justice Jon Roberts stated in the case of *Riley v California* (2024), "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought". Data protection involves principles, practice and

regulation that are targeted towards preserving the integrity, confidentiality and availability of personal information. Hence, with the way and manner technology evolves, societal shifts and legislative developments should follow suit. Recently, there have been a lot of data breaches, privacy scandals, cybercrimes and government surveillance. Alternatively, government has the responsibility to protect constitutionally guaranteed rights. For instance, protecting right to privacy entails personal information regarding a person is gotten appropriately, documented, used, retained and shared.

Civil liberties protection involves the protection of citizens' rights that are constitutionally guaranteed notwithstanding tribe, race, religion, gender or any other difference. It is important to draw a line between criminal activities and constitutionally protected activities. In our present world, it seems that technological innovation has outpaced privacy protections as governments can through its surveillance track one digitally. It is pertinent to state that as technology evolves, one's digital footprint is constantly growing with more information about the minutest details of our lives. For example, one's location, communication, online activities and many others can now be tracked and traced. Daily, citizens are constantly losing grip of their privacy and other information, while free speech, security and equality is also violated.

It is imperative to ensure that civil liberties are protected even as technological innovations progresses. Electronic information should also be protected at all cost as well as promote the proliferation of privacy-protection technologies. The protection of individual personal data is necessary as data becomes a valuable resource within the digital ecosystem. There is therefore the need for strong legal frameworks to address emerging risks of data misuse and ensure safety of individual personal information.

2. Research Questions

This paper seeks to examine the impact of digital technology on human rights and civil liberties. With a proper understanding of the emerging implications, governments across the globe can take adequate steps to strike a balance between technological advancements and protection of individual rights.

- Do digital innovations alter traditional expectations of how governments should protect rights in a digital era?
- Do digital innovations compound the balancing act necessary when faced with agitations between human rights?
- Are there ways data privacy can be compromised by government?
- Are digital rights same as human rights?

3. Privacy and Data Protection in an Information Era

Presently, ensuring and protecting citizens' right to privacy in the digital space is a significant concern given the rapid technological advancements. Many experts have expressed concern that the mass level privacy protection is weakening under the onslaught of digital technologies (Florimond, 2016). With the level of technological innovations, privacy and data protection is a necessary pre-requisite to ensure a safe haven for all. Presently, the use of various social media and online/internet platforms have afforded people the privilege of connectivity despite the distance. Thus, the level of processing of personal data in every phase of life makes it imperative that individual rights and privacy be protected at all cost in a modern era. (John Babikian, 2023) Privacy concern is topical and germane in this present contemporary society, hence the need to regulate and guard against the misuses of one's right or information provided on the internet. Privacy is one of the fundamental human rights that is recognized and respected in various international and regional documents. Privacy entails an obligation to keep the private life of an individual secret. The increasing cases of cyber theft, cyber-attack on personal data has necessitated a more stringent policies and laws to safeguard individual's privacy and respect user's data. The digital era facilitates novel ways by which people can exercise and enjoy their rights and new ways in which those rights can also be violated. This has raised a germane task for the government and stakeholders with respect to protection of interests peculiar to the digital context.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights provides for protection of people from "arbitrary or unlawful interference with one's privacy, family, home or correspondence and from unlawful attacks on one's honor and reputation. It went further to state that everyone has the right to the protection of the law against such interference or attacks. The latest resolution of the United Nations General Assembly with regards to right to privacy in this digital era was adopted by the Human Rights Council in 2019. It provides that States are under obligation to ensure that any interference with right to privacy is in line with the principles of legality, necessity and

proportionality. It provides that same rights people have offline must also be protected online including the right to privacy. It further provides that new technologies such as artificial intelligence can also impact the enjoyment of the right to privacy and other human rights. It is pertinent to state that this right to privacy under international human rights law is not absolute; however any form of interference must be backed up by law. Privacy entails two important rights namely; “right to privacy” and the “right to data protection”. The present digital age extend the privacy definition as a “privacy in the digital environment” or “electronic privacy” as discussed in the General Data Protection Regulation (GDPR). (Romansky & Noninska, 2020). Right to privacy is the very foundation of freedom of conscience, to be safe in one’s person and the right to reject self-incrimination. The first paradigm associated with right to privacy was defined in year 1890 (USA) by Samuel D. Warren & Loius Brandels in the article “The Right to Privacy” as a right to be let alone”, this constitutes part of the American precedent legislation. The nature and manner digital technology changes the way personal data are used, calls into question the basis of protection of personal online including consent to make use of personalized online content. For instance, the usage of individuals personalized post/content without authority or permission from the owner of such online post. Hence, it is brazenly clear that the extant policies on data and privacy protection are not sufficient to curb contemporary threats to individual privacy concerns.

On the other hand, personal data protection is also closely knitted and inter-connected with the privacy of individual’s personal information. Thus it involves a set of rules guiding the collection, storing, using, and dissemination of information about individuals. Personal data protection also involves the relations between persons and the society, presented by different subjects and authorities as government, state, institutions, public and private organization, companies; etc. Personal data processing must be based on stringent rules and regulations for data protection, and keeping privacy of the data subjects.

4. Digital Rights, Human Rights and Civil Rights

The technological innovations such as the Internet of Things, big data, cloud/ quantum computing, block chain technology and algorithms raises novel questions as to the use of such as well their regulation with respect to rights and protection of the citizens. The fact remains that digital technologies can violate several fundamental rights and rights provided in secondary legislation. The United Nations General Assembly in December 1966 adopted the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). The ICCPR treaty states that the right to privacy is a human right. The question is what is a human right? Human rights are those rights that simply inure to us because we are human beings. They are universally recognized rights by the State and are not granted by any State. They are universal rights available to all irrespective of nationality, sex, colour, ethnic origin, religion, and language or any other status and play a crucial role in political policies to protect every individual.(Sudrajat,2022) Another question that needs to be answered is; are human rights, digital rights? Digital rights basically are the fulfillment of human rights in the digital era. It is without doubt that the digital era introduced a lot of new technologies used for data analysis in real time, algorithms and data collections. Hence, there is no difference between human rights and digital rights

Access to the internet is the most basic digital right. Without it, implementing other rights in the digital space is impossible. J. Keane opines that only in countries with “communication abundance” such phenomena as “unelected representatives” and “cross-border public” have emerged (Keane, 2015: 206). By “unelected representatives”, Keane means the authoritative defenders of public interests and values, whose activities lie outside the plane of the legitimate electoral field. These can be bloggers, well-known writers, leading video blogs, and commenting on the situation with the censorship of the web and digital rights. The borderless nature and speed of digital technologies provides a novel avenue by which human rights can be exercised, violated or even abused. Digital technologies also afford people the opportunity to undermine the enjoyment of other constitutionally guaranteed rights and liberties and exacerbate individual and societal harms. For example, under section 39 of the 1999 Constitution of the Federal Republic of Nigeria, it provides that every person shall be entitled to freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information without interference. This is also obtainable in most civilized constitutions in the world. Hence, following from this provision of the law, citizens can exercise the right to expression or freedom of association online, or seek, receive and impart information and ideas through the internet. The striking question to ask is; to what extent is freedom of expression not interfering with the rights and freedom of others especially when the content is false, hateful or threatening. Hence, where unchecked exercise of the said rights above can result to cyber-attacks, misinformation and disinformation, violence and hostility and

sometime intentional interference with internet connectivity in critical times by government, these new forms of threat needs to be checkmated timeously.

In the era of social media and online content creation, freedom of speech is faced with a new challenge. The challenge whether restrictions are necessary to forestall the spread of harmful content or misinformation that can negatively jeopardize our society. Also, the accumulating data of citizens (their digital footprints) are collected and analyzed to identify consumer behavior patterns, the study of which is highly beneficial for platform owners (Srnicsek, 2020). Thus, the right to the inviolability of a citizen's private information sphere is made dependent on the interests and cyber policy of digital corporations. Here are some instance by which digital platform have influenced protection of human rights.

- Data and Privacy protection: Some personal individual information uploaded or shared are often used by either third parties or tech companies without obtaining the requisite consent from the persons concerned.
- Cyber bully and harassment: the anonymity prevalent in online and social media platforms encourages cyber bullying. Thus, people hide under the cloak of fake social media accounts to harass, threaten and bully individuals. This is in clear violation of human rights to security and protection from violence and insults
- Stiff response to security threats: sometimes government in order to maintain law and order may restrict online expression or stop access to the use of internet. This poses a threat to the right to freedom of speech.
- Quick dissemination of false information and hoaxes: the cyberspace provides a platform for quick spread of false or inaccurate information. This leads to unwarranted actions/reactions which can trigger riots, culminate into wrong actions or incite violence
- Freedom of speech: Social media and digital provides an avenue by which people air their opinions, and views on issues. Notwithstanding this, social media platforms impose community standards.

It is pertinent to note that any form of restrictions and regulation of the social media and freedom of speech and expression must be clearly based on rules that are specific and accessible. While ensuring adequate protection of personal liberty on social media, the right to freedom of expression must not be undermined. Because these freedoms are needed, it is paramount that they be written down in statute books that cannot easily alter. With regards to right to privacy versus security (whether individual or nation's security), to what extent can law enforcement agents interfere with the private lives of citizens. Actions such as surveillance, forensic examination and wiretapping strongly affect the right to privacy of an individual. Internet users are not only vulnerable to surveillance by private tech companies, but also to digital surveillance by governments who depend on tech companies and their digital tools to further their national security or law enforcement objectives. For instance, China has deployed facial recognition technologies in form of surveillance cameras that can identify individuals in real time, matching their personal data to video footage. It is submitted that this move may be considered as some citizens as overwhelmingly overreaching.

5. International Regulation/Protection of Digital and Data Privacy Rights

The relevance of privacy rights within human rights cannot be neglected. The collection of data like the browsing history, location, places visited; show an individual's identity and privacy rights. Hence, uncertainty as to how the data collected will be used, stored and possibly shared with third parties has the capacity of threatening an individual's right to control their personal information. On the other hand, identity theft on social media platforms, cyber stalking, cyber bullying and spreading of false information are common experiences that individuals face on a daily basis. This is generally as a result of the increase in the usage of digit services and platforms that are not adequately protected by law. (Mardiana, 2023) Given the pervasive nature of technological innovations in low and middle income countries, it is observed that legislations in some other jurisdictions like the United States of America and United Kingdom are proactive. While in countries like Nigeria and other Global South countries, legislations and policy guidelines are rather too slow.

Presently, there are three major countries vested with digital powers namely: E U, China and US. They are the leading countries in terms of regulating, and leading technology in the global digital order. They have demonstrated this by a coherent and well developed governance model for their digital economies. The US has pioneered a market driven model, China a state driven model and the EU a rights driven model. The EU model stresses the fact that digital transformation should be anchored on the supremacy of the rule of law and democratic governance. They opine that tech companies and government do not understand the pillars of

constitutional democracy or the fundamental rights of internet users. The EU firmly believe that regulatory intervention is necessary to uphold the fundamental rights of individuals, preserve the democratic structures and ensure a fair distribution of the benefits of digital innovations. The US is particularly concerned about protecting freedom of speech as a fundamental right. The EU seeks to balance the right to freedom of speech with other rights like right to privacy and human dignity. The Chinese government seeks to maximize the country's technological dominance while maintain social harmony and control over its citizens communications. This regulatory model adopted by Chinese government has been constantly criticized by democratic governments for using the internet as a tool for censorship and political control.(Bradford:) They ban and filter contents that are posted online, thus they portray the fact that freedom is not inherent in the nature of the internet but dependent on political choices by those in power who have the ability to limit freedom.

On the international scale there have been collaborations by countries targeted at protecting privacy and digital rights. The General Data Protection Regulation is an European Union law aimed at regulating how companies and organizations use, process and transfer personal data. It came into force on May 25th 2018 in all member states in order to harmonize data privacy laws in European countries. There is also the European Data Protection Board charged with the supervisory responsibility of coordinating signatory countries. The EDPB is made up of European Data Protection Supervisor and the EU national data protection authorities. In the US there is no single general legislation for protection of data, however there are numerous laws regulating that both at the federal and state level. Some federal data sector specific legislations include; Driver's Privacy Protection Act 1994, Children's Online Privacy Protection Act 1998 and the Video Privacy Protection Act 1988. In the US, states adopt data breach notification legislation that is peculiar to its residents. It is to be noted that while some states are less active, other states are more active than others when it comes to data protection.

6. Challenges of Regulating Internet/Online Violations of Digital Rights and Civil Liberties

Widespread Censorship and Monitoring: Countries of the world has as its priority to protect their cyberspace from terrorism and its likes. Thus in a bid to maintain peace and order in the polity, States employ electronic surveillance on the cyber space so as to foil any national security threat most times and not basically to protect individual citizen's rights. Mass surveillance and censorship is one of the ways artificial intelligence can infringe on human rights. A lot of risks associated with artificial intelligence have bearing on the enjoyment and exercise of human rights, including but not limited to privacy, equal protection under the law, freedom of opinion and expression and freedom of peaceful assembly and association.

- Lack of Effective Regulation: Most countries of the world do not have specific sector regulators that are charged with regulation of the
- Incessant rise of Cybercrime, Online Abuse, and Hate Speech.
- Unrelenting Spread of Disinformation or Misinformation
- Non-Compliance to Human Rights Regulation by Tech Companies: The main driver of digitalization is not states but large technology companies pursuing their own interests and profit maximization. Presently, there are new concepts related to the activities of technology companies in the digital environment for example "platform capitalism" by N. Srnicek (Srnicek, 2020), "surveillance capitalism" by S. Zuboff (Zuboff, 2019), "media imperialism" by O. Boyd-Barrett (Boyd, 2018). According to N. Srnicek, digital platforms that provide citizens with communication arenas for communication and exchange of opinions are interested in increasing the number of users. Digital platform owners' poses considerable risks to digital rights compliance, namely, are merging the revenue function with the oversight function.
- Digitalization and the introduction of "smart" digital technologies have generated several effects, to which it is important to draw the attention of policy makers and specialists in the area of protecting personal rights (Popova et al., 2021). The formation of the digital space of social and political communications has given a new sound to the issues of the implementation of traditional personal rights and freedoms that have been formed in democratic regimes over the centuries.

7. Conclusion

Technological innovations and advancements have ha progresses geometrically much more that the laws and policies regulating them. As digital transformation transcends into significant realizable gains, it is imperative, as it is with all innovations to be embraced with the requisite caution and attention with a view to

understanding its effect on all economic factors. Data privacy is a human right that is being recognized globally, this right enures to us by virtue of being humans. It is important that this fundamental and constitutionally guaranteed right should never be sacrificed at the expense of technological innovations and advancements.

Emerging approaches reveal that what constitutes rights in a digital era is compartmentalized and has implications on the coherence of efforts to promote them. Technological advancements and innovations have progressed geometrically much more than the laws and policies regulating them. Drawing from international human rights treaties and bodies, human rights have to be protected offline and online at all times. Hence the government across the globe needs to up their game and actions in ensuring the continued protection of human rights, constitutionally guaranteed liberties, as well as individual interests. Thus the aim of this paper is to analyze the connection between the emerging contemporary technologies, data protection and privacy in this digital era *viz-a-viz* human rights and civil liberties.

There is an urgent need for re-awakening among nations in enacting legal frameworks that are specifically geared to address the impact of digitalization on the enjoyment and protection of rights and on the interplay between them. Some countries may want to address these concerns using extant legal frameworks, while other countries may employ specific laws, policies, strategies and even novel rights that are geared towards individual's activities in a digital environment. It is expected that countries will enact a comprehensive and sustainable policy framework that will make room for the ever evolving nature of digital era to yield positive results for the society as a whole. It is paramount that individual's rights to data privacy be prioritized and strong security measures and end to end encryption be implemented.

8. Recommendations

- There is an urgent need for domestic, regional and international harmonization of data privacy and protection legislation, given the highly inter-connected and globalized world we are in.
- It is imperative that regulators and policymakers take into specific context, laws that are holistic and risk-based targeted at shielding the consumer from threat/ attack.
- Effective implementation of consumer protection laws which ultimately should promote the consumer by provision of these end-to-end encryption, data minimization, limited access, prompt notification of privacy policies in simple and understandable language.
- In some advanced climes, technology-related rights have been introduced to support digital rights particularly for artificial intelligence in countries like Japan and United States of America
- In an attempt to redress the negative effects of technology like digital inequality and the potential misuse of technology for harmful purposes, it is imperative for policy and law makers to prioritize human rights principles.
- There is also need for collaboration and synergy among technological companies, government agencies, civil society, online platforms and citizens in addressing this menace. This is a challenge that needs cross-sector and holistic approach so as to provide a safe and inclusive digital environment in line with best principles of human rights.
- In the European Union, General Data Protection Regulation and Data Portability grants individuals the right to request the deletion of their data from systems or to transfer their data from one service to another. This is also part and parcel of an individual having control over their data.
- Public education/sensitization and creation of awareness.
- There should be a requirement to give express, explicit and full consent by individuals before their personal can be used.
- There is need for network protection by service providers against external viruses, Dos attacks, data loss protection, web traffic filtering and protection of communication channels.
- In view of the novel technologies, it will be germane to have codified and integrated under state and regional laws, a new set of rights especially explicit digital rights. Rather than building or over stretching the already existing fundamental human rights, it will be most appropriate to have brand new set of rights. Some of the new digital rights includes; the right not to know, the right to be offline, the right to change your mind, and the right to safe digital environment.

References

Babikian J., Security Rights: Legal Frameworks for Privacy and Data Protection in a Digital Era", Law Research Journal (2023) Vol. 1, No 2

- Baker, S.M, Wade and Walsh M. (2020), "The Challenges of Responding to Misinformation during a Pandemic: Content Moderation and the Limitations of the Concept of Harm", Media International Australia, Vol.177 No 1. Available at <https://www//doi.org/1/77/ 329878X2095301>
- Gunjan Sharma, Dr. Abhinandan Bassai, Balancing Privacy and Innovation: Assessing Data Protection Laws in Modern Era", Supremo Amicus Vol. 35 May 2024
- Mardiana, N. & Meilan, A., (2023) Urgensi Perlindungan Data Pribadi Dalam Perspektif Hak Asasi Manusia. Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia 5(1). Available at <https://Doi.org/10.52005/Rechten.v5il.108>
- OECD (2022), Rights in the Digital Age: Challenges and Ways Forward", Available at <https://www.oecd.ilibrary.org>
- Office of the United Nations High Commissioner for Human Rights (2023) What are Human Rights? Available at <http://www.ohchr.org/en/what>
- Office of the United Nations High Commissioner for Human Rights(2023) "International Bill of Human Rights: A Brief History and the International Covenants" Available at <https://www.ohchr.org/en/what>
- Pittman, F.P., & Hafiz A., "Data Protection Laws and Regulations USA 2024., Available at <https://icig.com>. Accessed on 20 October, 2024.
- Romansky R.P., & Noninska, I.S., Challenges of the Digital Age for Privacy and Personal Data Protection", Mathematical Bioscience and Engineering (2020) Vol7 No.5
- Siagian R, Siagian Leonard, & Hamzah M.I (2023) Human Rights in the Digital Era: Online Privacy, Freedom of Speech and Personal Data", Journal of Digital Learning and Distance Education 2(1) 548-558
- Social Media and Human Rights: Issue Discussion Paper Commissioner for Human Rights (2021)
- The White House Fact Sheet: Advancing Technology for Democracy, Available at <https://whitehouse.gov>. Accessed on 20th October, 2024
- This strategy for Digital Council of Europe's Work in Progress. Available at: <https://www.coe.int/en/web/artificial-intelligence/work-in-progress>. Accessed on: November 21, 2024