(2023) 32 JUUM 25 - 35
https://doi.org./10.17576/juum-2023-32-03

ICT Omnipresence and the Rights to Privacy

Abdulkadir Bolaji Abdulkadir*
Abdulrazaq Owolabi Abdulkadir

ABSTRACT

The development of technology and online communication has also led to the appearance of what seem to be certain new types of criminal activity. Cyber security faced difficulties as a result of the rise in criminal behavior and the potential for the creation of new types of criminal activity online. This study evaluates the value of cyber security in an effort to stop cybercrimes based on this assumption. The research methodology used in this work is triangulation, which entails using many approaches to corroborate findings. The goal of this essay is to strike a balance between the requirement for cybersecurity and cybercrimes prevention and the right to privacy.

Keywords: Omnipresence; ICT; security, right; privacy

INTRODUCTION

The Internet is undoubtedly one of the most rapidly developing human sectors in terms of technical infrastructure. Evidently, information and Communication Technologies (ICTs) has become a common phenomenon today, and digitalization is becoming a more popular trend.[1] Products that previously ordinarily operated without the usage of computer technology are now being incorporated due to the ongoing desire for Internet and computer connectivity.[2] An instance of this is seen in vehicles and structures[3] which could typically operate without computers. However, this trend is rapidly shifting in the modern era, although the development of new technologies is mostly centered on satisfying the needs of consumers in western nations, developing nations could potentially profit from new technologies.[4]

In essence, the impact of ICTs in our society goes beyond building the foundational infrastructure for information. The development in the creation and use of network-based services was supported by the availability of ICTs. It is saying the obvious that emails have replaced conventional letters (although, this is not without effects on the human resources of the various postal agencies), just as printed marketing collateral has fallen out of favor in favor of online web representation, the latter being more crucial for businesses. Due to the quicker growth of phone services, obviously, internet-based communication has displaced landline communications. ICT accessibility and innovative network-based services have a lot of benefits for society as a whole, especially in developing nations. Some ICT applications including e-government, e-education, e-commerce, e-environment, and e-health are viewed as development enhancers since they all offer effective channels to deliver a wide range of fundamental services in isolated and rural locations. Applications of ICT can help reduce poverty in underdeveloped nations, achieve Millennium Development Goals, and improve health and environmental circumstances. When compared to services provided outside of the network, Internet services are less expensive. For instance, compared to traditional postal services, e-mail services are frequently offered for free or at very low cost. Hundreds of internet hosting services, including the free online encyclopedia Wikipedia, are also available for use without cost. Lower prices are crucial because they make services accessible to many more customers, especially those with low incomes. Internet facility and access have become easier for individuals, especially in poor nations with low financial means, therefore the Internet gives them access to services they might not otherwise been privileged. In this regard, online identity theft has continued threatening the deployment of e-government and e-business services, which is the act of intercepting another person's credentials and/or personal information via the Internet. This is mostly done with a view to fraudulently reuse it for criminal purposes. The present idea of the information society has evolved as a result of the integration of ICTs into many facets of daily life. Great opportunities are presented by this information society growth. Since the flow of information is no longer under

the authority of the government, unrestricted access to information can support democracy (as has happened, for example, in Eastern Europe and North Africa).[5] Daily life has been made better by technological advancements. Online banking and shopping, the use of mobile data services, and voice over Internet protocol (VoIP) telephony are just a few instances of how far ICT integration has come.[6]

However, new and significant concerns are emerging along with the development of the information society. Internet services and information infrastructure have already been the target of attacks. A few examples of the numerous computer-related crimes that are routinely committed on a large scale include online fraud and hacking attacks.[7] According to reports, cybercrime has a huge financial impact. Malicious software alone resulted in losses of up to USD 17 billion in 2003. According to some estimates, cybercrime took in more than USD 100 billion in 2007, surpassing the illicit drug trade for the first time.[8] It has been observed that nearly 60% of American firms have firm believes that cybercrime costs them more money than could be envisaged in actual crime. This assertion may be difficult to contradict and it is borne –out of their experiences in recent times. For example, in November, 2022, a United States District Judge Otis D. Wright II, sentenced one Ramon Olorunwa Abbas, a 40-year-old Nigerian national, whom is also known a "Ray Hushpuppi", 11 years in prison and to also pay $1,732,841 in restitution to two fraud victims.

The figures identified above, unequivocally show how important and crucial to safeguard both domestic and foreign information infrastructures. As a result, states at all levels have acted in the battle against cybercrimes by establishing legislation to prevent them. According to this viewpoint, Nigeria is not excluded from the conflict.[9] To stop cybercrime in Nigeria, the National Assembly established the Cybercrimes Act. The scope of this paper does not, however, allow for a thorough study of the offenses established by the Act; instead, it focuses on defending the right to privacy and defining its boundaries in the context of Nigeria's fight against cybercrime. This paper is broken down into six main sections. The first part is this introduction, which established the tone for the entire work. The notion of cybercrimes is examined in the second section in order to comprehend what it includes. The final section examines cybercrimes in Nigeria with the goal of highlighting the urgency of taking immediate action. The relationship between cybercrimes and cyber security is examined in the fourth section. This essay's fifth section examines the ideas of the right to privacy and cyber security in an effort to strike a balance between the two. The right to privacy is examined in the sixth section in light of the Cybercrimes Act. The conclusion is the last section.

UNBLOCKING THE CONCEPT OF CYBERCRIME

The absence of a uniform and all-encompassing legal definition for the behaviors that may qualify as cybercrime is a major issue for the analysis of cybercrime. This is because cybercrime can be described in a variety of ways, hence, conceptualizing it can be challenging. Computer-related crime, information technology crime, computer crime, electronic crime, and Internet crime are some of the other names for the concept. The purpose of this section is to give background information on the concept, *simpliciter*. Therefore, it is not within the realm of this paper to discuss the legal arguments surrounding cybercrimes. As a result, defining any of the aforementioned concepts will serve as a definition of cybercrime if the two are synonymous. Computer-related activities are just as prone to crime and just as likely to result in victimization as common physical crimes.[10] There are many different perspectives on what constitutes cybercrime because the types of crimes that are today being committed online occurred long before the internet was created. Two definitions of cybercrime—one that refers specifically to computer crime and another that refers to all forms of cybercrime—were created during the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders. According to its limited definition, cybercrime includes any illicit activity directed at the security of computer systems and the data they process through electronic methods.[11] In a broader sense, cybercrime (sometimes known as computer-related crimes) is any illicit activity carried out on or in connection with a computer system or network, which includes 13 offenses; to wit: providing or disseminating information using a computer system or network, as well as illegal possession (Carter, 1994). Cybercrime is defined more explicitly in some definitions which take into cognizance, objectives or intentions. For instance, "computer-mediated activities that can be carried out through worldwide electronic networks and that are either illegal or regarded illegitimate by certain parties."[12]

These more precise descriptions do not include instances where typical crimes are committed using actual gear. The categorization of cybercrimes has been used by some. For example, four categories of cybercrime have been established in the Council of Europe's Convention on Cybercrime (2001):

1. Crimes involving the confidentiality, integrity, and accessibility of computer data and systems;
2. Crimes involving computers;
3. Crimes involving content; and
4. Crimes involving the infringement of copyright and related rights.[13]

The multiplicity of approaches and associated issues show that there are many challenges in defining the term "cybercrime." The term "cybercrime" is used mainly to refer to a variety of offenses, including both network and conventional computer crimes. Cybercrime therefore, is a concept that does not necessarily exist, principally because there is no agreed-upon definition of it. This is made even more apparent by the fact that different jurisdictions have different definitions of crimes. Hence, the definition of the term "cybercrime" depends on whether it is broad or narrow. If a specific definition is chosen, cybercrime will only be understood to refer to offenses committed online while using a computer. Although not always including the use of the internet, a broad definition of cybercrimes will also cover other computer-related offenses.

CYBERSECURITY AND CYBERCRIME: REFLECTIONS ON THE LINKS

In a world that is interconnected, cybercrime and cyber security are concerns that are hard to be separate. The fact that cybercrime is mentioned as one of the key challenges in the UN General Assembly's 2010 resolution on cyber security, gives credence to this assertion. The continued and indeed the non-stopped advancement of information technology and internet services depend heavily on cyber security. Each country's security and economic health depend on enhancing cyber security and safeguarding vital information infrastructure. The new normal of government is to make the Internet safer (and safeguarding users of the Internet), because a safer internet is crucial to the creation of new services and government policies. A national cyber security and critical information infrastructure protection policy must include deterring cybercrime. This specifically entails the adoption of appropriate legislation to prevent the misuse of ICTs for illegal or other purposes, as well as actions meant to compromise the integrity of critical national infrastructures. At the national level, this is a shared responsibility that necessitates coordinated action from government authorities, the private sector, and citizens in relation to prevention, preparation, response, and recovery from incidents. This requires collaboration and coordination with pertinent partners at the regional and global levels. Thus, a comprehensive strategy is needed for the development and implementation of a national framework and strategy for cybersecurity. Cybersecurity measures such as the creation of technical defense mechanisms or user education to shield them from becoming victims of cybercrime can aid in lowering the risk of cybercrime. In the battle against cybercrime, the creation and support of cybersecurity strategies are essential. A crucial component of a cybersecurity strategy is the creation of appropriate legislation, and within this framework, the creation of a legal framework related to cybercrime. In order to make actions like computer fraud, unlawful access, data interference, copyright breaches, and child or criminal codes as presently constituted may not properly address cybersecurity. The Cybercrimes Act in Nigeria was passed as a result of this awareness; nevertheless, a study of it is outside the subject of this work. Advocates for civil society and others now recognize the potential negative effects that comprehensive pornography illegal, this necessitates the requisite substantive criminal law requirements. The fact that there are provisions in the penal code that apply to similar conduct committed outside of the network does not imply that such laws also apply to acts committed online. The most important question in this situation is when a state can intrude on someone's privacy in the interest of maintaining cybersecurity. This will be covered in more detail in the following section of the paper.

THE RIGHT TO PRIVACY AND CYBER SECURITY

Respecting human rights and fundamental freedoms while taking into account the protection of our data, security, and privacy in the digital sphere is what is meant by privacy.[14] On the one hand, it is the right to information and communication in cyberspace, and on the other, it is the right to security and privacy in cyberspace.[15] International standards and definitions define privacy as a personal and private area where we can use our skills and abilities and develop our personalities.[16] Numerous

international treaties and agreements mention the right to freedom. It encompasses the freedom to voice or express opinions as well as the freedom to seek and disseminate knowledge and ideas without interference from the government.[17] This right also includes the freedom to communicate and express oneself through any means, including words, deeds, images, and visuals, as well as through physical actions and the sharing of ideas and thoughts via social media or other online forums to protest against wrongdoing.[1819] The challenge will be to assess how human rights can be fully guaranteed under these arrangements and agreements.[20] The complete lack of proper data protection will have negative effects and repercussions on both the public's ability to exercise their right to human rights and the ability to leverage the realization of those rights. According to Clarke, privacy has been divided into the following magnitudes for a better understanding in relation to this study:[21]

1. Personal privacy, also referred to as "bodily privacy." This is connected to the person's physical integrity;
2. Personal behavior privacy. This applies to several facets of behavior, but especially to delicate topics like sexual proclivities and habits, political views, and religious beliefs, both in private and in public. It includes what is occasionally referred to as "media privacy."
3. The secrecy of private communications. This has to do with people's freedom to communicate with one another through a variety of mediums without routine monitoring by other people or organisations. Included in this are two things ("interception privacy") and
4. Personal information privacy: their right of control over their personal data and how it is used. They are also asserting their right that information about them should not be accessible to other people or organizations. This is also known as "information privacy" and "data privacy."

According to Clarcke, the last two listed factors are those most closely linked to cyber security because of the tight relationship that has developed between computing and communications, particularly since the 1980s. Several national and international human rights documents safeguard the right to privacy. For instance, every person must be safeguarded in terms of the right to protection from abusive attacks on their honor, reputation, and private and family lives based according to Article 5 of the American Declaration of the Rights and Duties of Man.[22] Additionally, everyone has the enjoyment of the right to life and the security of his or her person under Article 1 of the same Declaration. Here, the phrase "security of his person" also refers to "person privacy."[23] In Article 12 of the Universal Declaration of Human Rights, a person's right has described to mean protection of right privacy is protected.[24] The Declaration further stated that everyone has a right to legal protection from such meddling. It is interesting to note that the Cairo Declaration on Human Rights in Islam of 5 August 1990 openly and unequivocally supports a right to privacy for every person. Article 18 stipulates:[25]

> "Everyone is entitled to the freedom to practice their religion, care for their dependents, uphold their honor, and own their property. Everyone has the right to privacy in how they conduct their personal business, at their home, with their family, and in regards to their possessions and relationships. Spying on him, keeping an eye on him, or damaging his reputation are all prohibited. He must be shielded against arbitrary interference by the State. Private property is never infringed upon. It will not be unlawfully entered, destroyed, confiscated, or have its occupants evicted without the consent of the home's occupants."

No one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or communications, nor to unlawful attacks on his or her honor or character, according to the International Covenant on Civil and Political Rights' Article 17.[26] This covenant is crucial for having a clear knowledge of how our rights to freedom and privacy are protected in cyberspace.[27] If there are any limitations on these rights, that is the question at hand. The right to privacy in the Covenant does not include any equivalent constraints, in contrast to other clauses where they do. For instance, Article 19 of the ICCPR guarantees the freedom of speech and the right to express one's beliefs. However, under paragraph (3) of Article 19, various restrictions were imposed, including those regarding the protection of national security and the observance of other people's rights. This also reflects the proper interpretation of Article 18 of the ICCPR, which protects the freedom of religion and thought. The upshot of this is that one can draw the conclusion that the right to privacy as protected by the ICCPR is a fundamental freedom to which there are no limitations.[28] In fact, Article 5 of the ICCPR states that only the limitations set forth in the document may be enforced. It should go without saying that the ICCPR has no restrictions on the right to privacy. The key issue in this case

is how the court will handle the right to privacy under the ICCPR. However, the next section of this chapter will consider the court's disposition to right to privacy. Furthermore, the right to privacy is expressly guaranteed in the Nigerian Constitution. For instance, the Constitution's Section 37 provides as follows:

"The privacy of citizens is hereby guaranteed and preserved, including that of their houses, mail, telephone calls, and telegraphic communications."

The right to privacy was limited by the Nigerian Constitution, not by the ICCPR. In light of this, Section 45 of the Constitution states that no law passed in the interest of defense, public safety, public order, public morals, or public health will be deemed illegal by reason of Section 37.[29] It is asserted that these exceptions justify the Cybercrimes Act, which was passed to guarantee cyber security.

Article 8 of the ECHR states the following, which is analogous to Section 37 of the Nigerian Constitution:

1. Everyone has the right to respect for their home, correspondence, and private and family lives.
2. A public authority may not impede the exercise of this right unless doing so is legal, necessary for a democratic society, and serves the interests of national security, public safety, economic prosperity, the prevention of disorder or crime, the protection of health or morals, or the preservation of the rights and freedoms of others.

It merits mentioning that reservations similar to those of Nigeria are made and included in the second section of the ECHR.[30] Even though some states have not yet ratified these accords, all of these human rights are universally acknowledged, and the majority of them have evolved into accepted norms of international human rights law. This means that even while some international treaties have not been ratified by governments, many of these human rights still hold true and are still applicable, i.e., within national jurisdiction. They are customary and widespread because the vast majority of people follow them or incorporate parts of them into their national laws or legal processes. In the end, they are all binding both online and offline, and when they are violated both online and within physical space and borders, there is no distinction. In today's world, cyber security is essential, but so is the protection of one's right to privacy. Thus, it is necessary to strike a balance between the two. By doing this, cybercrimes can be avoided without needlessly infringing on an individual's right to privacy. This will be covered in more detail in the following section of the article.

NIGERIA CYBERCRIMES ACT AND THE RIGHT TO PRIVACY

The purpose of this sub-theme is to highlight the instances in which the government may be allowed to intrude on an individual's right to privacy. One of the reasons for such latitude is to protect online security and prevent cybercrimes. The sub-theme will examine some key provisions of the Nigerian Cybercrimes Act that protect personal privacy and their limitations.

DATA PROTECTION

Section 6 of the Cybercrimes Act forbids anyone from entering another person's computer system without their consent in order to gather or obtain information. Section 9 contains a similar clause that forbids unauthorized access to another person's data. In particular, the provision of section 21 of the Act requires a service provider to keep and maintain all traffic data and subscriber information as may be required by the relevant authority/agency in charge of overseeing the regulation of communication services in Nigeria at the time. Authorities like Economic and Financial Crimes Commission, Department of State Service, National Intelligence Agency, among others are the relevant authorities in this regard.

Importantly, to protect people's privacy, it becomes expedient to promise not to release such information without first getting permission from the data's owner. Law enforcement agencies like those mentioned above are only permitted to retrieve such information for a legal reason. Even at that a law officer is required by section 21(5) of the Act to give proper consideration to the individual's right to privacy, in doing so, under the Federal Republic of Nigeria Constitution of 1999. Recently, the Inspector General of Police in Nigeria warned his officers and men to desist from intruding into the hand phones of citizens. In fact, some officers have been dismissed as a result of failure to heed the directive. This is because the right to privacy is inextricably linked to data protection. The provisions of Section 21 of the Act have two major exceptions. First, private information cannot be

accessed by individuals or business entities without owner's prior permission and second, deduction is an exception that allows a law enforcement official to obtain private information only when necessary and not at will. However, the Act has made a crucial omission as to what constitutes a valid purpose as it is not even defined. This paper therefore argues that the Constitution provides specified instances in which access to private information may be seen to be made for lawful purposes. This argument is premised on the idea that since the right to privacy is inextricably linked to data protection, any restrictions on this right also restrict data protection. For instance, section 42(3) of the Constitution contains certain exceptions for the defense of the general welfare and public safety:

"Nothing in subsection (1) of this section shall invalidate any law by reason only that the law imposes restrictions with respect to the appointment of any person to any office under the State or as a member of the armed forces of the Federation or member of the Nigeria Police Forces or to an office in the service of a body, corporate established directly by any law in force in Nigeria."

The basic tenets of data protection legislation cover the gathering, registering, storing, using, and/or disseminating of personal data. The phrase "personal data" refers to information about specific natural or physical persons that can be used to identify them (and sometimes groups or organizations).[31] To ensure data protection, some fundamental guidelines have been acknowledged. In terms of the right to privacy, this presupposes that the government and its organizations cannot access and or tamper with an individual's personal information for the purpose of preserving cyber security and preventing cybercrime. Essentially, to assert one's right to privacy, it needs be stressed that one must adhere to the established norms in an effort to strike a balance between these two issues. Some fundamental guidelines on this subject, for instance, have been developed under the OECD Guidelines, which are:[32]

1. Personal data should only be collected legally and fairly (referred to as the "fair collection principle" below).
2. The "use limitation principle" states that personal information should only be used with the consent of the data subject or with valid legal justification.
3. Security measures should be put in place to protect personal data from unintended or unauthorized disclosure, destruction, or modification (hereinafter referred to as the "security principle").
4. Personal data should only be collected for specific and legal purposes and should not be processed in ways that are inconsistent with those purposes.

Regarding the automatic processing of personal data, the aforementioned standards are identical to the fundamental guidelines included in the Council of Europe Convention for the Protection of Individuals.[33] These tenets are condensed in Article 5 of the Convention. Before the question of privacy can come up, the aforementioned guidelines must be followed. As a result, it is impossible to claim that someone's right to privacy was infringed when they were prohibited from using data for improper purposes. The UN Human Rights Committee via General Comment 16 stated that Article 17 of the European Convention requires the legal discharge of essential data protections for private and public sectors to demonstrate the urgency of the need to secure data protection. An idea of what was proposed:[34]

"The relevant public authorities should only be permitted to request such information relating to a person's private life where having that knowledge is necessary for upholding society's interests as recognized by the Covenant. [...] The acquisition and storage of personal data on computers, data banks, and other devices by public authorities as well as by private people and organizations must be governed by the law. States must take effective measures to guarantee that information about a person's private life does not fall into the hands of people who are not legally permitted to receive, process, and use it, and that it is never used for goals that are inconsistent with the Covenant. Every person should have the right to know in an understandable manner if, and if so, what personal data is maintained in automatic data files, and for what objectives, in order to have the most effective protection of his or her private life. Every person should be able to find out which public authorities, private persons, or other organisations currently control or have the potential to control their files. Every person should have the right to ask for the correction or deletion of such files if they contain inaccurate personal data or were obtained or processed in violation of the law."

According to the Human Rights Committee's aforementioned statement, Article 17 of the ICCPR also includes data protection rights. The appropriate query in this situation is the determination of the violation to the Article. A person's privacy will only be invaded in violation of Article 17 of the ICCPR if it is done arbitrarily. Here, the term "arbitrary" refers to actions not supported by valid legal suppositions or grounds. This means that as long as a breach of a person's right to privacy is neither arbitrary nor illegal, it is acceptable under international human rights law. Therefore, even though the government

cannot intrude on an individual's privacy with regard to the information kept or personal data stored. The government must ensure that action is carried out for legitimate reasons. Hence, if a person provides the state with completely false information in order to commit computer-related crimes or offenses, the state may intrude on that person's privacy. In the case of *Cantrell v Forest City Publishing Co*,[35] the court held that in accordance with the law governing the right of party to safeguard and control their personal information, private persons are entitled to compensation for privacy intrusions when newspapers erroneously publish inaccurate information about them.[36]

INTERCEPTION OF CORRESPONDENCE

Section 7 of the Cybercrimes Act considers it illegal to intercept communications of a person. Any person who intentionally intercepts non-public computer data, content data, or traffic data using technical means, including but not limited to electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting signals, to or from a computer, computer system, or connected system or network, is said to be guilty of an offense, according to the provision of the law.[37] The phrase "unlawful", presents one of the section's biggest problems. This implies that there would not be any accountability in cases when the interception was legal. This is one of the areas where the Act is deficient in defining what illegal interceptions are all about. The Act in Section 22 does, however, give the required authorization to intercept communications, but only with a judge's permission.[38] The court must, therefore, be persuaded that interception is the best option available in this case.

Non-interference with communication is one of the main elements of the right to privacy. The Human Rights Committee emphasized, in its General Comment number 16, that in order to comply with article 17 of the International Covenant on Civil and Political Rights (ICCPR), it was necessary to guarantee both, the de jure and de facto, confidentiality of correspondence. In other words, correspondence should be delivered to the recipient without interruption, without being opened, and without being read in any other way. To guarantee the confidentiality of correspondence, states are under obligation, going by law, to offer protection against interfering with it. In issues involving the rights of convicts to private correspondence, the UN Human Rights Committee (HRC) has provided an elucidation of the correspondence privacy. For instance, the HRC ruled in *Angel Estrella v. Uruguay* that prisoners should be permitted, under the necessary supervision, to regular correspondence with their families and respectable friends without any hindrance.[39] There are some restrictions on this right, nevertheless, under the European Convention on Human Rights. The implication of this is that the authority may withhold any correspondence without being judged to have violated a person's right to privacy if doing so serves the interests of national security, public safety, or the country's economic well-being, or to avoid disruption or crime.

Also, in the case of *S v Nkabinde*,[40] The South African Court determined that the police had infringed the accused person's right to privacy by listening while his attorney was communicating with him.[41] The Monitoring Act does not cover the interception of this kind of communication, despite the fact that permission had been obtained under that Act. Furthermore, the monitoring had continued after the authorization's expiration date.

PRIVACY AND COVERT SURVEILLANCE

One can hardly conceive a state activity more detrimental to an individual's privacy than electrical surveillance, according to a famous statement made in the Canadian case of R v. Duarte.[42] The right to respect for private life, which is protected by the majority of international and regional human rights agreements, is the one that is most obviously under jeopardy within the context and contemplation of governmental surveillance. Article 8 of the European Convention on Human Rights (ECHR), for instance, states that "Everyone has the right to respect for their home, communications, and private and family lives." According to Articles 8(1) and 8(2) of the ECHR, a public authority may not impede the exercise of this right unless doing so is considered legal, necessary for a democratic society, and serves the interests of national security, public safety, economic prosperity, the prevention of disorder or crime, the protection of health or morals, or the preservation of the rights and freedoms of others.

The right to privacy is protected by section 37 of the Nigerian Constitution, which is also pertinent in this context. In accordance with the Constitution,[43] "The privacy of citizens is hereby guaranteed and preserved, including that of their houses, mail, telephone calls, and telegraphic communications."

Section 45 of the Constitution specifies the following restrictions on the application of section 37:

"Nothing in section 37, 38, 39, 40 and 41 of the Constitution shall invalidate any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health or (b) for the purpose of protecting the rights and freedom of other persons".[44]

This indicates that a state can only intrude on a person's privacy through determinable reasons known to the law. The justifiable reasons must, however, adhere to the limitations outlined in section 45 of the Constitution. In light of this, it may be claimed that section 45 has had the effect of ensuring the establishment of a thorough legal framework governing covert surveillance techniques, which must be used for legitimate reasons.

In addition, everyone has a right to legal protection from arbitrary or illegal intrusions into their privacy, which is specifically stated in the second paragraph of Article 17 of the International Covenant on Civil and Political Rights. This indicates that any communications relating to monitoring program must be carried out in accordance with a publicly available statute, which in turn, must be compliant with domestic and international human rights law and the State's own constitution. In the context of cyber security, such enabling law must not only be publicized but also be sufficiently specific to allow the person who will be impacted to control his or her behavior in anticipation of the potential implications of a certain activity. Any interference with the right to privacy, family, home, or correspondence must be permitted by rules that the State must make sure are in place:

1. are open to the public;
2. have clauses ensuring that the gathering, access, and use of communications data are tailored to specific legitimate aims; and
3. are sufficiently specific, laying out in detail the precise conditions under which any such interference may be permitted, the authorization process, the categories of people who may be subject to surveillance, the time limits for surveillance, and the use and storage procedures.
4. offer strong abuse prevention measures.

SEARCHES

Section 27 of the Cybercrimes Act allows law enforcement agencies to search any location or mode of transportation while investigating an offense made possible by the Act.[45] But before starting such a search, a few requirements must be met. One of these requirements is that a warrant be in place to authorize the search. The court's order must be obtained in that direction, which is the second prerequisite.

The International Covenant on Civil and Political Rights' provision in Article 17 provides safeguards against meddling in personal, domestic, and correspondence matters. An individual is shielded from unauthorized searches and seizures by the first two. In its remark number 16, the Human Rights Committee advised against harassing suspects during searches of someone's house and instead limiting them to gathering required evidence. For instance, in *Rojas Garcia v Colombia,*[46] the author's home was raided by the Colombian police under duress while they appeared to be targeting the wrong residence. The Human Rights Committee determined that the raid amounted to an arbitrary intrusion on the family's home despite the State Party's thorough arguments supporting the raid's legality.

CONCLUSION

Law enforcement agents are allowed under the law to invade individual's privacy, but this is subject to fulfillment of certain conditions. Individual's right must be based on numerous human rights provisions identified in this paper. Respecting or adhering to stipulated provisions of the law will curtail clamor for fundamental breaches pinpointed in this paper. Some law enforcement agents in an attempt at obtaining private data, disregard the law. Nigeria must be founded on a society free from crime in order to create a conducive environment for economic development. However, a perfect economy is essentially unimaginable because crime rates rise along with technology. Therefore, cybercriminals will always stay abreast of any technical advancement. While it is undeniable that technology contributes to cybercrime, it is ultimately up to us to decide how this country will develop in the future. On this note, the paper noted that it is very difficult to strike a balance between cyber security and the right to privacy. It is understood that the Cybercrime Act generally handles privacy and protection of data. The Act addresses varieties of cyber-related crimes and protect people's privacy.

NOTES

1 Abdulkadir, A. B. & Abdulkadir, A. O., 'Cybercrimes Act in Nigeria: Experimenting compliance with internationally recognized human rights provisions', (2019) 15 *Journal of International Studies*, p 119.

2 D.L. Carter, 'Computer Crime Categories: How Techno-Criminals Operate', (1995) *FBI Law Enforcement Bulletin,* http://www.fiu.edu/~cohne/Theory%20F08/Ch%20 14%20- %20Types%20of%20computer%20crime.pdf [1 March 2023].

3 S. Charney, 'Computer Crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace', (1994) 41(7) *Federal Bar News,* p 469.

4 C. Hale, 'Cybercrime: Facts & figures concerning this global dilemma', (2002) 18(65) *Crime & Justice International,* http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 [7 October 2019].

5 O. Emmanuel, 'Elbit Systems officials arrive, begin installation of $ 40 million internet spy facility for Nigeria', *Premium Times*, 26 November 2013, https://www.premiumtimesng.com/news/150333-exclusive-elbitsystems-officials-arrive-begin-installation-40-million-internet-spy-facility-nigeria.html [7 October 2014].

6 O. Emmanuel, 'Elbit Systems officials arrive, begin installation of $ 40 million internet spy facility for Nigeria'.

7 A. Rushinek & S.F. Rushinek, 'Using experts for detecting and litigating computer crime', (1993) 8(7) *Managerial Auditing Journal,* p 19-22.

8 D. Simpson, 'Feds Find Dangerous Cyber stalking Hard to Prevent', *CNN,* 12 June 2000, https://edition.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/index.html [14 July 2017].

9 Anon, 'Types/Incidences of Cybercrime in Nigeria', *Martins Library,* 2013, http://martinslibrary/blogspot.com/2013/08/type-incidence-of-cybercrime-in-nigeria.html [14 July 2017]. See also Anon, 'Florida Cyber-Security Manual', *Secure Florida,* 2004, https://secureflorida.org [7 October 2019].

10 Anon, 'Types/Incidences of Cybercrime in Nigeria' and Anon, 'Florida Cyber-Security Manual'.

11 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, p 5, https://www.uncjin.org/Documents/congr10/10e.pdf [1 March 2023].

12 C. Hale, 'Cybercrime: Facts & figures concerning this global dilemma', (2000) 18(65) *Crime & Justice International,* http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 [7 October 2019].

13 See http://www. conventions.coe.int.Treaty.

14 J. Jarvis, 'A Bill of Rights in Cyberspace', *Buzz Machine*, 27 March 2010, http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace [7 October 2019]. See also K. Rodriguez, 'Internet Surveillance and Free Speech: the United Nations Makes the Connection', *Electronic Frontier Foundation*, 4 June 2013, https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection [7 October 2019].

15 J.P. Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, 8 February 1996, https://www.eff.org/cyberspace-independence [7 October 2019].See also 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc. Doc. A/HRC/20/L.13. Human Rights Council, 29 June 2012, para.1.

16 'Report of the World Conference on Human Rights by the UN Secretary-General', UN Doc, GA A/CONF.157/24 (Part I), October 1993 http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En [14 July 2017].

17 H. Nissenbaum, 'Toward an approach to privacy in public: Challenges of information technology', (1997) 7(3) *Ethics & Behavior*, p 207-219. http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf [7 October 2019].

18 'Human Rights Indicators: A Guide to Measurement and Implementation',Office of the High Commissioner for Human Rights, 2013, https://unp.un.org/Details.aspx?pid=23745 [1 December 2018]. For the definition of digital rights see Ranking Digital Rights project. Business and Human Right Resource Center. http://www.business-humanrights.org/Documents/Ranking_Digital_Rights [1 December 2013].

19 F. Hare, 'Borders in cyberspace: Can sovereignty adapt to the challenges of cyber security?' in C. Czosseck & K Geers, K. (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* IOS Press, Amsterdam, 2009.

20 J. Arquilla & D. Ronfeldt, 'Cyberwar is Coming', (1993) 12 *Comparative Strategy,* p 141-165.

21 R. Clarke, 'What's 'Privacy'? Workshop at the Australian Law Reform Commission, 28 July 2006, http://www.rogerclarke.com/DV/Privacy.html [14 July 2017].

22 American Declaration of the Rights and Duties of Man 1992.

23 Warren and Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol. IV, Dec 15, 1890, No. 5. S.D. Warren & L.D. Brandeis, 'The right to privac', (1890) 4(5) *Harvard Law Review*, p 193-220.

24 W.L. Prosser, 'Privacy', (1960) 48 *California Law Review*, p 383-423. http://dx.doi.org/10.2307/3478805. For a broad survey of the right to privacy, see generally R.C. Turkington A.L. Allen, *Privacy Law: Cases and Materials,* 2nd Edn, West Group, St. Paul, 2002.

25 Cairo Declaration on Human Rights in Islam, (UN Doc A/45/421/5/21797, 199).

26 International Covenant on Civil and Political Rights 1966.

27 See M.R. Konvitz, 'Privacy and de Law: A Philosophical Prelude', (1966) 31 *Law and Contemporary Problems*, p 272-280 for a discussion of the historical development of a right to privacy beginning with Biblical and ancient Greek conceptions.

28 See generally E. Goffman, *Behavior in Public Places,* Free Press of Glencoe, New York, 1963; E. Goffman, *The Presentation of Self in Everyday Life*, Anchor Books/Doubleday, New York, 1959; C. Fried, C., 'Privacy', (1968) 77(3) *The Yale Law Journal*, p 475-493.

29 *See* City of Santa Barbara v. Adamson, 610 P.2d 436, 439 (Cal. 1980) ("The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose.")

[30] J.M. Devlin, 'State Constitutional autonomy rights in an age of Federal retrenchment: Some thoughts on the interpretation of State rights derived from Federal sources', (1990) 3 *Emerging Issues in State Constitutional Law*, p 197.

[31] L. Irwin, 'The GDPR: What Exactly is Personal Data', *IT Governance,* 22 March 2022, https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data [4 February 2023].

[32] There are four relevant instruments in this respect: (i) the CoE Convention on data protection (see *supra* No. 1); (ii) the EC Directive on data protection (see *supra* No. 2); (iii) the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data (Paris: OECD, 1980), adopted 23.9.1980; and (iv) the UN Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990), adopted by the UN General Assembly on 4.12.1990. Of these, only the first two listed are legally binding instruments. Note, however, that the CoE Convention does not require a CoE member state to implement its provisions until it is ratified by the state. A range of international instruments have also been adopted dealing with data protection for specified sectors of activity, but only one of these instruments is legally binding: this is the EC Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (OJ No L 024, 30.1.1998, 1), adopted 15.12.1997.

[33] See the Council of Europe Convention for the Protection of Individuals, with regard to automatic processing of personal data (ETS 108). See also the Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), Strasbourg, 28.I.2003

[34] Human Rights Committee of the United Nation, comment 16. See further, see J.G. Merrills, *The Development of International Law by the European Court of Human Rights,* 2nd Edn, Manchester University Press, 1993, p 18–19.

[35] 419 US (1967).

[36] 419 US (1967).

[37] See Cybercrimes Act 2014

[38] Ibid.

[39] *Angel Estrelle v Uruguay* (74/80).

[40] 1998 8 BCLR 996 (N).

[41] (*S v Nkabinde*1998 8 BCLR 996 (N)

[42] (1990 65 DLR (4th) 240, at 249).

[43] Constitution of the Federal Republic of Nigeria 1999 [as amended] 2011.

[44] See the following cases: (*Malone v UK* (1984) 7 EHRR 14, *Leander v Sweden* (1987) 9 EHRR 433). In *Kruslin v France* ((1990) 12 EHRR 546).

[45] See the Cybercrimes Act 2014.

[46] *Rojas Garcia v Colombia (687/96).*

REFERENCES

Abdulkadir, A.B. & Abdulkadir, A.0. 2019. Cybercrimes Act in Nigeria: Experimenting compliance with internationally recognized human rights provisions. *Journal of International Studies 15*: 119.

American Declaration of the Rights and Duties of Man 1992.

Anon. 2004. Florida Cyber-Security Manual. *Secure Florida*. https://secureflorida.org [7 October 2019].

Anon. 2013. Types/Incidences of Cybercrime in Nigeria. *Martins Library*. http://martinslibrary/blogspot.com/2013/08/type-incidence-of-cybercrime-in-nigeria.html [14 July 2017].

Arquilla, J. & Ronfeldt, D. 1993. Cyberwar is coming. *Comparative Strategy* 12(2): 141-165. https://doi.org/10.1080/01495939308402915.

Barlow, J.P. 1996. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*, 8 February. https://www.eff.org/cyberspace-independence [7 October 2019].

Berlin, I. 1958. *Two Concepts of Liberty*. Oxford: Clarendon Press.

Cairo Declaration on Human Rights in Islam, (UN Doc A/45/421/5/21797, 199).

Carter, D.L. 1995. Computer Crime Categories: How Techno-Criminals Operate. *FBI Law Enforcement Bulletin*. www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20- %20Types%20of%20computer%20crime.pdf [1 March 2023].

Charney, S. 1994. Computer Crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace. *Federal Bar News* 41(7): 489.

Clarke, R. 2006. What's 'Privacy'? Workshop at the Australian Law Reform Commission, 28 July. http://www.rogerclarke.com/DV/Privacy.html [14 July 2017].

Constitution of the Federal Republic of Nigeria 1999 [as amended] 2011.

Crimes related to computer networks. 2000. Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, A/CONF.187/10. http://www.uncjin.org/Documents/congr10/10e.pdf [1 March 2023].

Devlin, J.M. 1990. State Constitutional autonomy rights in an age of Federal retrenchment: Some thoughts on the interpretation of State rights derived from Federal sources. *Emerging Issues in State Constitutional Law* 3: 197.

Emmanuel, O. 2013. Elbit Systems officials arrive, begin installation of $ 40 million internet spy facility for Nigeria. *Premium Times*, 26 November. https://www.premiumtimesng.com/news/150333-exclusive-elbitsystems-officials-arrive-begin-installation-40-million-internet-spy-facility-nigeria.html [7 October 2014].

Fried, C. 1968. Privacy. *The Yale Law Journal* 77(3): 475-493.

Goffman, E. 1963. *Behavior in Public Places*. New York: Free Press of Glencoe.

Goffman, E. 1959. *The Presentation of Self in Everyday Life*. New York: Anchor Books/Doubleday.

Goodman, M.D. 1997. Why the policy don't care about computer crime. *Harvard Journal of Law & Technology* 10(3): 466-494.

Hale, C. 2002. Cybercrime: Facts & figures concerning this global dilemma. *Crime & Justice International* 18(65). http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 [7 October 2019].

Hare, F. 2009. Borders in cyberspace: Can sovereignty adapt to the challenges of cyber security? In Czosseck, C. & Geers, K. (eds.). *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press.

Human Rights Indicators: A Guide to Measurement and Implementation. 2013. Office of the High Commissioner for Human Rights, https://unp.un.org/Details.aspx?pid=23745 [1 December 2018].

International Covenant on Civil and Political Rights 1966.

Irwin, L. 2022. The GDPR: What Exactly is Personal Data. *IT Governance,* 22 March. https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data [4 February 2023].

Jarvis, J. 2010. A Bill of Rights in Cyberspace. *Buzz Machine*, 27 March. http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace [7 October 2019].

Kiskis, M. 2011. Entrepreneurship in Cyberspace: What do we know? *Social Technologies* 1(1): 37-48.

Konvitz, M.R. 1966. Privacy and de Law: A Philosophical Prelude. *Law and Contemporary Problems* 31: 272-280.

Merrills, J.G. 1993. *The Development of International Law by the European Court of Human Rights*. 2nd Edn. Manchester University Press.

Nissenbaum, H. 1997. Toward an approach to privacy in public: Challenges of information technology. *Ethics & Behavior* 7(3): 207-219. http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf [7 October 2019].

Prosser, W.L. 1960. Privacy. *California Law Review* 48: 383-423. http://dx.doi.org/10.2307/3478805.

Ranking Digital Rights project. Business and Human Right Resource Center. http://www.business-humanrights.org/Documents/Ranking_Digital_Rights [1 December 2013].

Report of the World Conference on Human Rights by the UN Secretary-General. 1993, UN Doc, GA A/CONF.157/24 (Part I). http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En [14 July 2017].

Rodriguez, K. 2013. Internet Surveillance and Free Speech: the United Nations Makes the Connection. *Electronic Frontier Foundation*, 4 June. https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection [7 October 2019].

Rushinek, A. & Rushinek, SF. 1993. Using experts for detecting and litigating computer crime. *Managerial Auditing Journal* 8(7): 19-22.

Simpson, D. 2000. Feds Find Dangerous Cyber stalking Hard to Prevent. *CNN,* 12 June. https://edition.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/index.html [14 July 2017].

The promotion, protection and enjoyment of human rights on the Internet. 2012. UN Doc. Doc. A/HRC/20/L.13. Human Rights Council, 29 June.

Turkington, R.C. & Allen, A.L. 2002. *Privacy Law: Cases and Materials*. 2nd Edn. St. Paul: West Group.

Warren, S.D. & Brandeis, L.D. 1890. The right to privacy. *Harvard Law Review* 4(5): 193-220.

Abdulkadir Bolaji Abdulkadir* (Corresponding author)
Associate Professor
Department of Public Law
Faculty of Law
University of Ilorin, Nigeria
E-mail: abdulkadir.ba@unilorin.edu.ng

Abdulrazaq Owolabi Abdulkadir
Associate Professor
Department of Private and Property Law
Faculty of Law
University of Ilorin, Nigeria.
Email: kadir.or@unilorin.edu.ng