LEGALITY AND JUSTIFICATION OF THE RIGHT TO INTERCEPTION IN EAST AFRICAN COUNTRIES: A COMPARATIVE ANALYSIS OF CYBER LAWS

Innocent Pius Kibadu[1*]

"Lawful interception is a powerful tool to fight crime, but it is an equally powerful tool to commit crime, if the necessary protections are not available."

Abstract

The right to interception under the world of information technology is frequently undertaken by the government agencies to prevent crimes committed under cyberspace. Cyber laws in some East African countries inadequately protects the right to communication of individuals, groups or organisation procedural wise. Absence of judicial approval of procedural provisions relating to interception leads to questionability of its process thereof. This article explores the legality and justification of the right to interception in three East African Countries namely; Tanzania, Kenya and Uganda under cyber laws. The exploration hinges on the competing interest between the right to privacy and the right to interception for public interests in cases like crime prevention and detection; and safeguarding the national security. The discussion concludes that the right to privacy cannot overlap the public interests; and interception under cyber laws is inevitable. However, in terms of procedures, judicial approval for interception order should be clearly stated in the cyber laws. Keeping abreast of accommodation of human rights is the striking balance between the two competing interests.

Key words: *Interception, Cyberspace, Cybercrimes, Privacy, Public Interest and National Security*

1.0 Introduction

Governments worldwide do intercept individual's communication in the course of government administration or enforcement of its laws. Historically, interception goes back in the United Kingdom (UK), where it was not recognised and later recognised under a statutory regime when the *Interception of Communications Act, 1985* (ICA), was enacted and turned the history in the case of *Malone v. Commissioner for the Metropolitan Police (NO.2)*.[2] In this case, the *European Court of Human Rights* (ECHR) held that the English practice of interception was insufficiently grounded in law to allow it to be justified under the European Convention on Human Rights, specifically *Article 8*, which protects the individual against arbitrary interference by public authorities in his private or family life.[3] Thus, interception infringes right to privacy and personal life of an individual. In the case of *Lambert v France,*[4] the European Human Rights Court stated that the interception of telecommunications represents an interference with the right to privacy under the European Convention.

However, in certain circumstances individual's communication may be intercepted by the government under justifiable reasons or cause in securing the national interests. Indeed, normally interception is authorised in matters which are regarded as subjecting in danger the national security or disturb the public order in a country. In the circumstance as such, the State through its law enforcement agencies may intercept one's communication to prevent endangering situation in plan.

If interception is done without the consent of a person, or lawful cause, the act amounts to a cybercrime. That once interception is committed, it must be legally acceptable and justified under the laws. This article aims at examining the legality of right to interception and its justifications under cyber laws in the three East African Countries. The discussion will cover analysis of cyber laws available in Tanzania, Kenya and Uganda.

1.1 Defining Concepts

Before going into detail discussing the most part of the theme of this article, there are concepts which are of paramount importance to understand as they build a cornerstone of the article's argument. The understanding of the concepts involved in this discussion will ease and lead the reader to grasp the intended knowledge conveyed by the author.

1.1 Interception

There is no single universal consensus definition of the concept of interception. Variably, the meaning of which mainly is drawn by the practice exercised by each government.[5] Forexample, Amanda Hale and John Edwards define interception as:-

> *A person intercepts a communication in the course of its transmission if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication.*[6]

Various jurisdictions define interception in the contexts of their laws. For instance, the *Tanzania Intelligence and Security Service Act*[7] defines interception as:-

> *any communication not otherwise lawfully obtainable by the person making interception, includes hear, listen to, record, monitor, or acquire the communication, or acquire its substance, meaning or purport.*[8]

1 * The author of this article is an Assistant Lecturer in Law-Tumaini University Makumira, Mbeya Centre. He holds LLM-ICTLAW and LL.B; Mobile: 0756 864 851 / 0717312657; E-mail: *innocentkibadu@gmail.com*

2 [1979] 2 All ER 620; *see also*, Philip Ward and Alexander Horne, (2015), *"Interception of Communications,"* at p.1.

3 The London School of Economics and Political Science, *Briefing on the Interception Modernisation Programme*, Houghton Street, London, PEN paper 5, at p.7

4 (2000) 30 EHRR 346 [21]

5 Executive Committee of the High Commissioner's Programme, "Interception of Asylum-Seekers and Refugees: The International Framework and Recommendations for a Comprehensive Approach," *A Paper presented at the 18th Meeting of the Standing Committee,* (EC/50/SC/CPR.17), 9th June 2000, at p.3

6 Oxford Pro Bono Publico, *Legal Opinion on Intercept Communication,* United Kingdom; University of Oxford Project, January, 2006, at p. 7.

7 [R:E 2002]

8 S. 2, *Ibid*

On the other hand, the new Tanzanian cybercrimes law, define the term interception in relation to a function of computer as:

> *acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device;*[1]

That the two statutory definitions cited above defers depending on the purpose and goals aimed at to be achieved by the specific law.

However, interception can be described as the interception of communications in the monitoring and scrutiny of private messages between individuals or organisations. Likewise, interception may be referred to as a right to or interest in accessing constrained intentional observation which is persistent one, of one's activities by others.[2] The earliest obvious form is the reading of the mail.[3] Today, interception is advanced where voice communication may be intercepted as well. Such interception activities can be done by an individual person privately or by the government through technical support as public interception.

Therefore, once interception perpetrated by an individual is unlawful, and where it is conducted by the government can be lawful or unlawful one depending on whether the government is exercising a just or unjust interception. In certain circumstances, interception is perpetrated or interrupted against an individual's life especially the asylum seekers and refugees,[4] for various security reasons. Therefore, interception can be lawful or unlawful one. However, this article hinges its discussion on interception in the context of interception in communications.

1.1 Privacy

It refers to the ability of an individual or group of individuals to stop personal information from becoming known to people other than those whom they choose to give the information to.[5] That an individual claims to control his personal information not to be acquired, disclosed, used or identifiable to another individual without his consent thereto. The potential for wide-range of interception of all our cyber-activities today, presents a serious threat to information privacy of an individual.

1.1 The Right to Interception

The concept of *"right to interception"* is complex one in the sense that it involves violation of the right to privacy by intercepting ones communications in the information technology era. The term *"right"* in itself should not be confused with the phrase *"human rights."* Further, in this context the term *"right"* should not be taken for granted. It should be understood into a philosophical point of view. Hegel argues that right is positive generally if it has validity in a state with established authority which is the principle for the knowledge of right.[6] This takes us to the understanding that it is the State that knows which act is a right and which one is not a right. In relation to *"right to interception"* it implies that the State through its agencies has the right to intercept ones communications as it is acknowledged that it is a right to intercept one's communication for a particular purpose(s).[7] On the other hand, it demonstrates that an individual person or entity without any legal justification once intercepts one's communications; it is regarded as an illegal interception in the eyes of the law in the first place.

1.1.1 Cyberspace

Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication such wires. Kang in his paper, defines cyberspace as the rapidly growing network of computing and communication technologies that have profoundly altered our lives.[8] David on the other hand, maintains that 'cyberspace suggests a computerized dimension where we move information about and where we find our way around data.'[9]

1.1.2 Cybercrimes

At a glance, it is pertinent to note that there is no universal agreed definition of the phrase cybercrimes. Thus, each individual country defines it depending on the scope and purpose of the legislation in question. However, different scholars have defined the term cybercrimes, but for the purpose of this article, it suffices to pick the leaf from the definition given by Jovan Kurbalija in his book titled; *An introduction to Internet Governance,* that cybercrimes includes unauthorised access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorised interception of data to, from, or within a system or network; as well as computer espionage.[10] The impact of the acts such as that is violation of individuals' rights such as right to privacy or privacy of the State would be jeopardized in case of computer data espionage.[11]

1.0 Rationale of Interception

Though interception is a breach of confidentiality of an individual's personal communication,[12] the right to privacy cannot override national security. It follows therefore that, interception can be perpetrated only by the State with justifications under the law; and not interception by an individual. However, in intercepting process, cooperation between the State organs and the service providers is a prerequisite requirement for each to perform its duty.[13] In addition to that, since interception under cyber space involves service providers on one hand, to avoid chaos, there should be no conflicting laws regulating the key players in interception.[14] There are some reasons for the State to intercept one's communication trail. The reasons include the following as discussed hereunder:-

2.1 Interests of the National Security

Basically, the national security refers to the state or condition where our most cherished values and beliefs, the democratic way of life, institution of governance and unity, welfare and wellbeing as a nation and its people are permanently protected and continuously enhanced by the government. Indeed, wherever there is jeopardizing situation or condition which is or likely to threaten the national security, then the government law enforcement agencies has a right under the law to intercept any communication in connection to the suspects so as to prevent the threatening situation or circumstances.

Normally, governments are vested with powers of ensuring security of the nation is safeguarded. To that effect, governments all over the world, through their law enforcement agencies such as the police, army and the intelligence units, daily are striving hard to protect their nations. Therefore, communications that may be taking place between individuals or certain organization to the extent that the exchanged communication jeopardises the national security can be intercepted by the government,[15] to safeguard public interests in terms of security and national tranquillity.

1 S.3 of the Cybercrimes Act, 2015
2 Kenyon, A. T and Richardson, M, *New Dimensions in Privacy Law: International and Comparative Perspectives*, New York; Cambridge University Press, 2006, at p. 145
3 *Ibid*
4 *Supra note* 3
5 Kamal, A. *The Law of Cyber-Space: An Invitation to the Table of Negotiations*, United Nations; Institute of Training and Research, 2005, at p. 1 3
6 Hegel, G.WF. *Philosophy of Right*, (Translated by .W Dyde), Canada; Batoche Books Limited, 2001, at p. 23
7 Consider the interception done unnoticeable by the State Intelligence and Security Services in various jurisdictions.
8 Kang, J. "Information Privacy in Cyberspace Transactions," *Stanford Law Review,* Vol. 50, 1998, at p. 1193
9 Koepsell, D. R. "*The Ontology of Cyberspace: Questions and Comments,"* Department of Philosophy and School of Law, State University of New York at Bufalo, (unpublished), at p.5.
10 Jovan Kurbalija, *An introduction to Internet Governance*, 6th edn., DiploFoundation, 2014, at p.103
11 Currently, Russia has been accused by the USA of intercepting general election tallying system to enable Dolnad Trump to win the election.
12 Kenyon, A. T and Richardson, *supra,* at p.24
13 Rogialli, C., "Today's Challenges in Lawful Interception," *A Presentation Paper Presented at RIPE Meeting 51 –Amsterdam,* October 11, 2005, at p. 5
14 The service provider laws should also provide for provisions relating to interception enabling the enforcement agencies to intercepting.
15 The interception must be legally provided under the law

It should be born in our mind that interception of communications is one of the investigative techniques that are manifested by intelligence units and law enforcement agencies mainly to meet specific reasons, namely; safeguarding the national security interests, for the prevention and / or detection of serious crime, and to safeguard the economic well-being of the government.[1] On the contrary, it should be noted that, the right to interception by the government do not supersede an individual's right to privacy. The right to privacy of an individual is constitutionally guaranteed at national and international levels. In fact, it is very difficult however to draw a clear cut line of demarcation between an individual's right to privacy and the State's right to intercept for both are protected under the laws. *Adrien Jammet* in his article points out and reiterates that:-

> *In reality, the digital world is not only a new social space that has been mostly created and organised by private entities, it also represents a new territory for the expression of human rights and the risks that it implies.*[2]

In the light of Adrien's assertion above, it is undeniable substantive fact that individual's right to privacy is a human right; and that right under cyber space is under risk of being violated in various ways such as interception of one's communication by the State. On the other continuum, national security may be jeopardized with ubiquitous use cyberspace. Therefore, national security and the right to privacy are two competing variables at risk. The question is which one overlaps the other? This question will be dealt in the later discussion.

There are other instances where military bases are attacked by hackers under cyberspace to steal security information by attackers from outside the country. This is evidenced by *Cliff Stoll* as quoted by *James A. Lewis* in his article in which he reveals that the Eastern bloc service (probably the KGB) hired a group of West German hackers to steal data from U.S. military computers. The West Germans connected remotely to university networks in the U.S. and used them for the attacks. They were finally tracked down and arrested, but they did not know who had commissioned them to do that.[3] Stoll's findings are further supported by Russinovich in his presentation paper arguing that "Computer systems at the Pentagon and other military sites get 'attacked' thousands of times each year."[4] This kind of attack apart from endangering the national security it is also a serious crime committed against the State. Thus, in an effort to protect the national security and wellbeing of the nation, interception conducted under cyberspace is inevitable in any developed and developing countries in the age of information technology.

2.2 Prevention or Detection of Serious Crimes

The right to interception bears a serious relationship with cyber laws when dealing with cybercrimes such as terrorism. Terrorism in most cases yields massive killing of the people, rape and other associated cybercrimes. It is in this regard, that interception is inevitable in preventing or detecting serious crimes as such.

Currently, the whole world is threatened with terrorist's activities which cost life of the people in a massive trend. In addressing this situation a number of jurisdictions have enacted anti-terrorists law so as to curb terrorist's activities including interception of communication in their jurisdictions should there be any sort of terrorist activity plotted to take place. Developed countries such as United States of American are the champions for interception as far as cybercrimes are concerned, terrorism in particular.

Interception under cyberspace can also be carried out by the government in detecting crimes through its law enforcement organs. Detection of seriousness of crimes is done after the crime has already been taken place. Thus, under the circumstances as such the investigative bodies may if they find reasonable to intercept communication of an individual or any other body purposely for detection of seriousness of the crime that have been committed, they intercept. Intercepting the communication under this aspect is of help in furthering criminal proceeding since detection of the crime open an opportunity for criminal activities to take place.[5]

However, interception of an individual's communication should be covered under the law which provides for the procedures for interception. The notion behind is that, since traditionally investigation procedures for search and seizure, law enforcers require a court warrant, then the same should apply in interception of communication.[6] This was reiterated in the case of *Katz* v. *United States,*[7] where the US Supreme Court held that electronic monitoring of a telephone call was a 'search and seizure' within the *Fourth Amendment*, meaning that interception without a warrant did not comply with constitutional standards. As such the court pointed out that 'reasonable expectations of privacy may be defeated by electronic as well as physical invasion.'[8] Therefore, justification for intercepting communication of an individual should be well versed under the law prescribing the procedures for intercepting. In doing so, the aspect of protecting human rights will be kept abreast within the black letters of the law.

2.3 Safeguarding the Economic Wellbeing of the Government

A number of economic activities for the nation nowadays are electronically transacted such as banking businesses, trading activities, communication services, and the like. Likewise, organised crimes such as sabotage, smuggling, terrorism, fraud, forgery and corruptions activities also are taking precision under cyberspace as well. Kaspersky report indicates that any business even a small business is not safe from cyber espionage.[9] That being the case, cyber laws providing provisions for interception is inevitable. Cyber laws providing for interception in preventing cybercrimes which are threatening the economy of a nation are very important at the expense of an individual's privacy of his or her privacy in communication. Frankly speaking, the national interest should prevail over individual's interests in the economic development of the nation and its citizens. In the recent celebrated case of *Jebra Kambole v Attorney General*,[10] citing the Parliamentary Hansard, the High Court of Tanzania quoted *inter alia* the objectives that:

> *to provide a framework for the protection of individual rights and freedoms against cybercrime; to provide for the mechanism and framework of combating cybercrime in Tanzania; to establish offences and punishments relating to cybercrimes in Tanzania and to outline rules and procedures for the investigation and prosecution of cybercrimes; to provide for the rules on the liability of service providers in relation to cybercrimes;* ***and to provide for protection of the national economy and financial services against cybercrimes****. [Emphasis supplied]*

Therefore, if individuals or organisations make their communications which are probably doubtful and injurious to the development of the economy of the country such as sabotage, corruption activities, smuggling, and the like, then the respective bodies of the government can intercept such communication so as to prevent the perpetrators from putting into action their evil plans to safeguarding the economic wellbeing of the nation. However, interception sought should not only be legally provided under the laws of a country as justification for doing the same but also procedures of doing the same should be clearly stipulated to avoid confusion and unnecessary resistance from the public and violation of privacy of an individual.

1 Rogialli, C., *supra,* at p.10
2 Jammet, A. "The Evolution of EU Law on the Protection of Personal Data," *Centre for European Law and Legal Studies, Online Paper Series*, No. 6, 3, 2014, at p.2
3 Lewis, J. A. "Computer Espionage, Titan Rain and China," *Center for Strategic and International Studies - Technology and Public Policy Program*, 2005, at p. 2 (Unpublished)
4 Russinovich, M, "Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon," A Presentation Paper Presented at RSA Conference, 2013, at p. 2
5 Lloyd, I. J. *Information Technology Law*, 6th edn., Oxford University Press, 2010, at p.264
6 Caloyannides, M. A. *Privacy Protection and Computer Forensics, 2nd edn.,* London; Artech House, 2004, at p.7
7 389 US 347 (1967).
8 Kenyon, A. T and Richardson, M, *supra,* at p. 146
9 Kaspersky Lab, *Special Report: Who's Spying on You? No business is safe from cyber-espionage*, 2013, at p.8
10 Miscellaneous Civil Cause No. 32 of 2015, at p.3 *(Unreported).*

2.0 Significance of Interception under Cyber Laws

States especially in developed countries such as the United States of America, German, China and other countries has developed their cyber capability for security and economic growth for their respective countries. In keeping pace against the competing countries, militarily and economically, these countries undergoes interception processes in other countries and steal information which are of paramount importance for them to advance their technology.[1] This is termed as cyber espionage.

Russinovich in his presentation paper indicates that States maintains and utilise cyber capabilities mainly for four reasons, namely:

> *(1) to deter other States by infiltrating their critical infrastructure;*
>
> *(2) to gain increased knowledge through espionage in cyberspace, which makes it possible for States to advance more quickly in their military development;*
>
> *(3) to make economic gains where technological progress has been achieved—for example, through industrial espionage; and*
>
> *(4) to be able to attack and paralyze an adversary's military capacity or the adversary's ability to control its own forces in a conflict.*[2]

Looking at the above cited reasons for cyber capability, we find that interception under cyber laws is of paramount importance, since cyber espionage aims at paralysing the economic and security strength of another nation. It follows that, as pointed out earlier that governments are vested with powers to ensure security of a nation, both economic and militarily, interception is justified on the party of the victim country. Indeed, countries through cyberspace platform must have operational cyber legal frameworks which provides for interception of electronic communication so as to detect and prevent cyber espionage from both internal and external attacks.

3.0 Legality and justification of interception

Legality and justification for interception of communication under cyber laws is recognised by having cyber laws which provide to the State with a substantive right to intercept. On the other hand, procedural provisions which provide for procedures on how interception of communication is to be carried out should be intact enshrined in the law. However, balancing the right to privacy and public interest should be taken into account during the legislative process of cyber laws regarding procedural matters.

4.0 The Right to Interception and Cyber Laws in East African Community

At the outset, it is important to note that this part analyses the right to interception and cyber laws in three countries in the East African Community (EAC), namely; Tanzania, Kenya and Uganda as aforesaid. It explore the extent to which the procedural aspect of the right to interception under cyber laws are legally provided and justified as against the right to privacy in communication as guaranteed in their respective constitutions as part and parcel of human rights. The analysis is seriatim extended in the order as hereunder:-

4.1 Tanzania

The legal framework on the right to interception under cyber space in the Tanzanian context is a bit controversial. Different laws have been enacted providing for recognition of the right to interception, its legality and justification in intercepting communication. In this subpart, three laws are examined hereunder focusing on the legality and justification for the right to interception by the government against individual, group or organisation.

1 USA spying drones sent in China
2 Russinovich, M. *supra* at p. 5

4.1.1 The right to interception under the Prevention of Terrorism Act

Rapid and increasing terrorist's activities that are taking place worldwide necessitated various jurisdictions to take initiatives and make anti-terrorist laws, Tanzania being one of them.[3] The purpose of enacting anti-terrorism law is to safeguard the national interest, that is, the national security against the terrorists and their activities. The objective of enacting the anti-terrorist law is clearly stated in the long title of the law which *verbatim* states that:

> *An Act to provide for comprehensive measures of dealing with terrorism, to* ***prevent and to cooperate with other states in the suppression of terrorism*** *and to provide for related matters. [Emphasis supplied].*

The law mainly centred and focused on detecting and preventing terrorists from subjecting the national security in danger. That in case government intelligence agency or unit secures any terrorists information, interception of communication connecting the terrorist's suspects is carried out to detect and prevent them from putting into action their terrorist evil plot. The enactment of this law has led to the amendment of the *National Security Act*,[4] which empowers the law to proceed with the proceeding under the anti-terrorism law. Many countries in the world have responded to the threats of terrorism and criminal activities by enacting legislation that provides the legal basis for lawful interception.[5]

5.1.1.1 Legality and Justification

The legality of the right to interception under anti-terrorist's law is immersed in the procedures given for intercepting communication under the law for various purposes including collection of evidence by a police officer.[6] That, justification sought is collection of evidence relating to a specific offence charged. A police office may after obtaining a written consent from the Attorney General;[7] apply to the court for an *ex-parte* order for interception of communication.[8] However, the law empowers the police officer to obtain interception order discretionary by using the phrase *"may apply."* The powers are likely to be misused by the police officers in implementation processes. The purpose of a warrant is to protect individuals from undue interference with their rights particularly the right to privacy. This is further thought to give a more objective basis of challenge by defendants and control by the courts. This position was reiterated in the United States of America, in the case of *People v Bialostok,*[9] where the State's Court of Appeals stated categorically that:

> *If a warrant is required by law, the fact that the officers behaved reasonably without one is unavailing. The purpose of the warrant requirement is to interpose a neutral and detached Magistrate between citizens and the police to protect individuals from having to rely on the good conduct of the officer in the field for the protection of their right to be free of unreasonable searches.*

The law empowers police officers with discretionary power to obtain a court order or warrant for interception of communication. However, in practice, the experience shows that, police officers full vested with discretion to obtain a court order or exercise a discretionary power, they choose to exercise a discretionary power conferred arguing that the matter in question needed an urgent action and without obtaining a court warrant. The extent of police officers in exercising discretionary powers conferred is questionable from one case to another. This is not good in a country which appraises to embrace good governance since it raises irritating questions as to the integrity of the intercepting officer against the interception subject. In many instances as such implications of violation of human rights such as the right to privacy is crucial.

3 *The Prevention of Terrorism Act, 2002* was enacted following the 1998 US Embassy Terrorist attack in Tanzania and Kenya
4 S. 10A of the National Security Act, Cap. 47 [R:E 2002]
5 Utimaco LIMS, *"Lawful Interception in the Digital Age: Vital Elements of an Effective Solution,"* White Paper, 2014, at p. 5
6 Police officer of or above the rank of Assistant Superintendent of Police
7 S. 31 (2) of the Prevention of Terrorist Act, 2002.
8 S. 31(1) *Ibid*
9 (1993) 594 N.Y.S.2d 701 (CA), 704

4.1.2 Interception under the Electronic and Postal Communication Law

This is another cyber law which provides for interception issues. It is the first cyber law enacted in Tanzania in 2010.[1] Since crimes can be committed under cyberspace, the law accommodated at least some traditional crimes to cybercrimes once committed electronically under this law. *The Electronic and Postal Communication Act (EPOCA)* prohibits unlawful interception; disclosure or attempt to disclose any information obtained through interception or use or attempt to use the intercepted contents of a communication.[2] The law further prohibits an authorized officer to disclose any intercepted content of communication.[3] However, the law indirectly recognizes interception of communication to an authorized officer, yet the law does not provide for the procedures of intercepting individual's communication. This is in line with *Makulilo's* argument that:

> *EPOCA is an interception law as it authorizes interception of subscribers' content of communication because it would be illogical for the Act to prohibit disclosure of the content of information which was not intercepted and retained in the first place.*[4]

Logically, there is no doubt in essence that individual's communications are intercepted without interception procedures accommodating judicial approval of interception recognized under this law. To make this serious, the government through the miscellaneous amendment law, it placed attempt or disclosure of intercepted communication as an economic and organised crime triable by the Economic and Organised Crimes Division of High court.[5]

1 No. 3 of 2010
2 S. 120 of the EPOCA, 2010.
3 S. 121, *Ibid*
4 Makulilo, A. B. "Registration of SIM Cards in Tanzania: A Critical Evaluation of the Electronic and Postal Communications Act 2010," *Computer and Telecommunications Law Review,* 2011, at p.4
5 S. 16 of the *Written Laws (Miscellaneous Amendment*) Act No. 3 of 2016; paragraph 37 to the First Schedule of the Economic and Organised Crimes Control Act, Cap 200 [R:E 2016]

Moreover, mandatory SIM card registration[6] is intended to establishment an extensive database of user information, eradicating all the potentials for anonymity of communications. The system enables mobile user location tracking, and simplifies communications surveillance and interception to be easy.[7] When these entire acts takes place without properly laid down procedures under the law, then violation of privacy of an individual is realized and the key actor is the government itself.

5.1.2.1 Legality and Justifications

The law regulating electronic and postal communication does not provide for procedures on how to intercept communication of an individual, though the same law prohibits unlawful interception and disclosure of intercepted contents of communication. In the situation as such the law is inadequately regulating interception activities. Thus, it indirectly provides discretionary power to law enforcement agency to require information intercepted, while on the other hand it is silent on the duty of the communication service providers to respond positively to the request received. If the law is silent on the provisions providing for procedures for interception though indirectly recognizing interception under the same law; then legality and justification of interception of communication is questionable.

The law also places the communication service providers under threat for being squeezed out of its licenses for it is the government itself who issues licenses. At this juncture, in most cases, the practice of police officers is obtaining intercepted information under friendly basis between one of the employees of the communication service providers and the police officer at the risk of the company being sued by the victim for violation of his right to privacy or under political pressure by the government in power or effective control by the government apparatus.[8] This is not healthy in country exposing itself to have been promoting and protecting its individuals from human rights violation.

6 S.131 of the EPOCA, 2010
7 Privacy International, *The Right to Privacy in Rwanda: Universal Periodic Review Stakeholder Report: 23rd Session, Rwanda*, March 2015, at p. 8.
8 *Jebra Kambole v The Attorney General*, *(Supra),* at p.2 *(Unreported).*

1.1.1.1 Interception under the Cybercrimes Act

Early April, 2015 Tanzania through the Parliament passed the new cybercrimes law and subsequently assented by the President of the United Republic of Tanzania. It came into force on the 01st day of September, 2015.[9] Interception of communication under this law is touched but not very much clear. The drafting of the provision relating to interception is similar to that of EPOCA in which it only provides for illegal interception but it is silent on the lawful interception. It also does not provide for procedures for lawful interception by a lawful authority. The law indirectly provides powers to law enforcement agency to intercept. Like anti-terrorism law discussed above, the new cybercrimes law is silent on the procedures for the same. That, the legality and justifications under this law is similar to that of EPOCA. Thus, this law also is not clear as to the legality and justification of the right to interception under cyber space. Further, certain offences under the *Cybercrimes Act* (including interception) are now triable under the Economic and Organised Crimes Division of High court.[10]

5.1.4 Observations under Tanzanian laws

Cyber laws in Tanzania with exception to anti-terrorism law are not clear on the procedures of intercepting communication of an individual. Since procedures are the ones which determine the legality for interception in the course of interception, then short of which renders the interception conducted unjustified. A good legal framework provides for both substantive and procedural provisions. Unclear procedures relating to interception results to bad practice of interception by the law enforcement agencies which in return lead to violation of the right to privacy. In the circumstance as such, Tanzania is viewed as among of the leading countries for illegal interception of individual's communication particularly in communication mobile phone. Accusations against the government are posed alleged of connecting wires to telecommunication companies directly in which the agencies are able to listen and record live conversation and even tract the whereabouts of the customer.[11] According to the report given by Vodafone, Tanzania is the fourth country in the number of phone interceptions among the reported countries with many data and voice interceptions. This was revealed by the Executive Director of Tanzania Consumer Advocacy Society (TCAS) in which he claimed to file a 90 days' notice to the government for violation of right to privacy.[12] Neither justifications have been sought for conducting such interception nor are procedures laid down under the law. Additionally, in Tanzania there is no specific law dealing with regulation of interception of communication such as Uganda. Multiple provisions relating to interception in different laws with variations of intercepting procedures lead to conflicting procedural standards or benchmarks I processing the same.

9 GN No. 328 of 2015
10 S. 16 of the *Written Laws (Miscellaneous Amendment*) Act No. 3 of 2016; paragraph 36 to the First Schedule of the Economic and Organised Crimes Control Act, Cap 200 [R:E 2016]

1.1 Kenya

Like other countries in the EAC, Kenya endowed with laws legalizing interception of communications. It is worth noting that, Kenya is currently and tremendously threatened and frequently attacked by terrorist's attacks from Al-Shaabab residing both in Kenya and Somalia. Therefore, intensive security precautions and measures traditionally and through ICTs have been constantly taken care of by the government of Kenya in securing the national security and its citizens. Infact, it is tantamount to note that, cyber attacks come from terrorists seeking to inflict political or economic damage.[13] Consider the Westgate and Garisa University terrorist's attacks,[14] the attacks apart of costing lives of the people, the attacks distorted the economic stretch and destabilized political atmosphere in Kenya

11 http://www.businesstimes.co.tz/index.php?option=com_content&view=article&id=3588:phone-interceptions-tanzania-to-land-in-court&catid=1:latest-news&Itemid=57[Downloaded on 10th/07/ 2015]
12 *Ibid*
13 Government of Kenya, Ministry of Information Communications and Technology, *Cyber Security Strategy*, 2014, at p. 4
14 In the year 2015

and the EAC as a whole.

5.2.1 The Kenya Information and Communication Act

This law prohibits any licensed telecommunication operator from intercepting a message sent through that telecommunication system while not in the course of its business.[1] Further, the law prohibits any person directly or indirectly to intercept or cause interception of any function of computer system.[2]

5.2.2 Interception under Mutual Legal Assistance Act

In the year 2011, Kenya enacted a law which provides for a mutual legal assistance to foreign country in investigation processes by intercepting communication of an individual suspect of criminal matter. This has been given under *Part VI* of the law. The justification for the provision of mutual legal assistance in interception is facilitation of criminal investigation requested by another country to Kenyan authority.

5.2.3 Interception under the Prevention of Terrorism Act

Kenya different from other EAC countries discussed above, is the last country to enact anti-terrorist law among the three countries under discussion herein. Although the law was enacted in 2012, still the law is inadequate in combating terrorism vide frequent terrorist attacks led to amendment of the same. In the year 2014, the government of Kenya waged a *Security Law (Amendment) Bill* and passed it to become a law to the effect that various security laws such as the *Prevention of Terrorist Act* are amended in response to prevention of terrorism.[3] The enacted law legalizes interception of communication focusing at detecting, deterring and disrupting terrorism.[4] However, the interception procedures under the law are mandatory vested to the Cabinet Secretary and approved by the National Assembly before being put into effect.[5] The law further justifies interception of communication at the expense of right to privacy on the grounds of detecting, deterring and disrupting terrorism[6] in the course of securing the nation and its citizens. It is pertinent to note however that, the amending law was brought aftermath of an increasing terrorists attacks perpetrated by a terrorist's group noticed as *Al-Shaabab* from the nearby politically unstable country, Somalia.

Noticeably, the law came into force on 22nd of December, 2014, but subsequently the law was challenged in the High Court under the Constitutional and Human Rights Division by way of petition in which the petition was moved by three Petitioners, namely; *Coalition for Reform and Democracy (CORD), Kenya National Commission for Human Rights and Samuel Njuguna Ng'ang'a v Republic of Kenya and the Attorney General.* The petition also involved eight interested parties and two *amicus curiae.*[7] The ruling was delivered on 23rd February, 2015. In the petition, the provisions have been challenged on the basis that they limit the right to privacy. With regard to the amendments to the *Prevention of Terrorism Act*, ARTICLE 19 (one of the interested parties) submitted that Section 69 of *Security Laws (Amendment) Act* - (SLAA) which introduced Section 36A to the *Prevention of Terrorism Act* is unconstitutional as it violates the right to privacy. The counsel, Mr. Mureithi's submitted that Section 36A introduces uncalled for mass surveillance of communication by all National Security Organs, which is unconstitutional. On the respondent side, averred that the core of the State's case with regard to the limitation of the right to privacy, as with the other provisions which have been assailed on the basis that they limit or threaten to limit fundamental rights, is that they are justified in the State's war against terrorism.

Mr. Muturi for respondent further submitted that the measures complained of were justified by the effect of terrorist attacks on innocent Kenyans in the recent past by illustrating enumerating number of terrorist attacks in the past few years: that there had been 20 attacks in the year 2011, 37 in 2012, 25 in 2013 and 30 in 2014. The court ruled *inter alia* that, *(at pp. 90-91):*

> *(i) The need to monitor communication permitted in both Part V of the National Intelligence Service Act and the Prevention of Terrorism Act, which it is conceded limit the right to privacy has one purpose; to enhance national security by ensuring that national security agents, through their covert operations and monitoring of communication, can be one step ahead of terrorists, and are thus able to thwart terrorist attacks. This, we are convinced, is an extremely important purpose, recognised world over as justifying limitations to the right to privacy;*
>
> *(ii) A right to privacy can never be absolute. It has to be balanced against the State's duty to protect and vindicate life. What needs to be done, to subject the limitation and the purpose it is intended to serve to a balancing test, whose aim is to determine whether the intrusion into an individual's privacy is proportionate to the public interest to be served by the intrusion;*
>
> *(iii) Judicial notice is taken of the numerous terrorist attacks that this country has experienced in the last few years,* ***we are of the view that the interception of communication and the searches contemplated under the two impugned provisions of law are justified and will serve a genuine public interest****. The right to privacy must be weighed against or balanced with the exigencies of the common good or the public interest. In this instance, the scales tilt in favour of the common good.* ***[Emphasis supplied]***

Picking the leaf from the ruling of the court in the above petition, it is my firm submission that the legality and justifications for interception of communications in matters threatening national security and the life of its citizens, public interest prevail against individual's interests such as privacy. Taking into account the frequent terrorists attacks directed to Kenya, there is no way interception of communication can be avoided in detecting, deterring and disrupting terrorism as sought by the law against any suspect. Besides, the terrorists on the other hand, are knowledgeable of being intercepted; they have reduced communication using mobile phones, instead they are communicating through encrypted messages, using e-mail draft boxes such as Dead Letter Boxes (DLB) and adopting use of such applications like *WhatsApp* social network.[8] This is another challenge in the war against terrorism and their activities in Kenya and the EAC at large.

5.2.4 Interception under the National Intelligence Service Act

Following the increasing terrorist's attacks directed to Kenya, it prompted the government of Kenya in response thereto, to take a move to enact the *National Intelligence Service Law* in 2012 which among other things, its goals was to provide for procedures of investigation in matters which are threatening the national security. *Part V* of the law provide for the procedures to be followed by the Director General before making an *ex-parte* application to a Judge of High Court for a warrant enabling the service to investigate on the matter.

5.2.5 Computer Misuse and Cybercrimes Act

Kenya among the three countries under discussion is the last country to enact the specific cybercrimes law. It is until May this year 2018 when Kenya enacted specifically the *Computer Misuse and Cybercrimes Act* which came into force on 16 May, 2018.[9]

1 S.31(a) of the Kenya Information and Communication Act, 1998 [R:E 2009]
2 S. 83 (b) of the Kenya Information and Communication Act [R:E 2009]
3 S. 69 of the Security Laws (Amendment) Act, 2014.
4 S. 36A(1) the Prevention of Terrorism Act, 2002
5 S. 36A(2), *Ibid*
6 S. 36A(3), *Ibid*
7 *Petition No. 628 of 2014 consolidated with petition no.630 of 2014 and petition no.12 of 2015;* See also, *Kenya Law Reform Commission, "Security Law Amendment Act Ruling,"* Available at http://www.klrc.go.ke [accessed last on 21st / 08/ 2015]
8 "Terrorism threat in the country," at p. 33; *Available at https://info.publicintelligence.net* [Accessed on 21st /08/ 2015]
9 Kenya Gazette Supplement No. 60 (Acts No. 5)

The law prohibits an individual to intercept electronic messages or money transfer unlawfully with intent to destroy or abort such communication.[1] However, the law also makes lawful interception of content data required for the purpose of investigation of an offence; and such interception must be done by a police officer or an authorized person.[2]

5.2.5.1 Legality and Justifications

The *Computer Misuse and Cybercrimes Act* provides for provisions regarding procedures and justifications for interception of content data. The law provides that the police officer or authorized person may apply to the court for an order to:-

> *(a) permit the police officer or authorised person to collect or record through the application of technical means;*
>
> *(b) compel a service provider, within its existing technical capability —*
>
> *(i) to collect or record through the application of technical means; or*
>
> *(ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system.*

In addition to an application sought by the applicant the law requires him to include certain information such as the reasons for believing possession of the content data in the computer system, type of content data, the offence in which the warrant is sought, state if he has authority of collecting such information, statement on maintenance of privacy of information to other users and non disclosure of information, state how investigation may be frustrated and state the manner in which the objective of the warrant will be achieved.[3] The scope of interception is limited to the period not exceeding nine months, subject to extension of time upon satisfaction by the court.[4] To ensure compliance of the law, the court is vested with a discretionary power to require the service provider to keep confidential the order and execution of any powers under the law.[5]

5.3 Observations under Kenyan Laws

Although the laws in Kenya legalizes and justifies interception of communication under cyberspace, it is arguably that the government of Kenya under its regulation[6] has conferred enormous power to the government organs to intercept communication of individual especially in collecting and accessing mobile phones data.[7] The regulation places an obligation to telecommunication service providers to grant access to their systems to the State authorities without judicial order. And the fact that interception process requires judicial approval, there are concerns that judicial processes are being circumvented and the privacy of citizens violated.[8] This echoes with the claim raised by Vodafone that in its Transparency report, *Law Enforcement Disclosure Report*, of June 2014, in which it revealed that it had *'not received any agency or authority demands for lawful interception assistance'* in Kenya. Thus, the inference drawn from this disclosure is that the Kenyan authorities have direct access to Vodafone's network, which allows the government to monitor communications directly without having to go to the telecommunication company to seek for the data of their customers.[9] This is a bad practice under the rule of law and good governance for Kenya in as far as the right to privacy is concerned.

1 S.31 of the *Computer Misuse and Cybercrimes Act, 2018*
2 S.53(1) *ibid*
3 S.53 (2) of the *Computer Misuse and Cybercrimes Act, 2018*
4 S.53 (4),(5) *Ibid*
5 S.53(6) *Ibid*
6 *See,* The Information and Communications *(Registration of Subscribers of Telecommunication Services)* Regulations, 2014
7 S. 13, *Ibid*
8 Privacy international and the coalition of Human right defence in Kenya, "The Right to Privacy: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence," *A Universal Periodic Review Stakeholders Report; 21st Session, Kenya*, at p.6
9 *Ibid*, at p.9

If the matter is legally justified, then proper procedures should be followed to follow the effect for national interest and vice versa.

On the other hand, the newly enacted law, *Computer Misuse and Cybercrimes Act* though provides discretionary to the police officer or authorized person to intercept content data in a computer system, it has also set a provision which prevent and control misuse of the conferred powers under the law. The law imposes a penalty to any police officer or authorised person who misuses the exercise of powers conferred under the law.[10]

1.2 Uganda

Uganda possesses a number of laws providing for matters of interception. The State has a system of intercepting all electronic communications and filter in and out of the country communications which are of terrorist in nature. In fact, this is done under the right to interception through prevention of terrorism laws.[11] Ideally, no government is ready to operate under insecure state. The State is duty bound to make sure that any sort of serious crimes as such are detected and prevented before aftermath.

5.3.1 Interception under Anti-Terrorism Act

The *Anti- Terrorism Act* vested a huge power to the authorized government officials to intercept any form of communication in the course of investigation of acts and obtaining information relating to terrorism by interception.[12] Indeed, justification for interception is enshrined in the law as the purpose of the right to intercept by the government are preserving the public interest, prevention of violation of the fundamental and other human rights and freedoms of any person from terrorism, preventing or detecting the commission of any offence under the Act; or safeguarding the national economy from terrorism.[13] Whereas the law also provides for wider scope of interception and powers conferred to authorized officers.[14]

5.3.2 Interception under the Computer Misuse Act

The *Computer Misuse Act* is another law in Uganda which addresses in a nutshell the issue of interception. The law categorically prohibits any person from intercepting or causing interception of communication directly or indirectly.[15] Though the law indirectly gives interception mandates to authorized officers, yet it provides no laid down interception procedures and justifications under the law. Therefore, its legality and justification regarding the right to interception is questionable.

5.3.3 Interception under the Ugandan Communication Act

The *Ugandan Communication Act* vehemently prohibits unlawful interception of communication of a person[16] on one hand; and it provides for lawful interception of the same on the other hand. The law further places liability to any communication operator or its employee who intentionally intercept government communication.[17] That it is only the government which is vested with powers or conferred with the right to intercept communication of an individual under the law. Like the *Computer Misuse Act*, the *Communication Act*, also indirectly provides for lawful interception, but no procedures and justification provided down under the law. It is insufficiently justifying interception by providing that there is a lawful excuse to intercept, but what constitutes a lawful excuse is not given or contemplated under the law, hence questionable in law.

5.3.4 Interception under the Regulation of Interception of Communications Act

Uganda went further by enacting the law

10 S.54(2) *Ibid*
11 African Media Barometer Uganda, *The first home grown analysis of the media landscape in Africa,* Windhoek, Namibia; Friedrich-Ebert-Stiftung, 2012, at p. 25; *See also*, *Part VII* of the Ugandan Anti-Terrorism Act, 2002
12 *See*, the Long Title and Part VII of the Ugandan Anti-Terrorism Act, 2002
13 *Ibid*, S. 19(4)
14 *Ibid*, s. 19(5) and (6)
15 *See*, s. 15(1) of the Ugandan Computer Misuse Act, 2011.
16 S. 79 of the Ugandan Communication Act, 2013
17 S.80, *Ibid*

specifically providing for procedures to be followed in conducting lawful interception of communication by government officials.[1] The law also establishes the interception monitoring centre which *inter alia* is charged with powers such as to acquire, install and maintain connection between the telecommunication systems and the centre; and that is to be monitored by the centre itself.[2] This law seems to provide interception procedures and regulate interception of all interceptions given in other laws so far as they are dealing with communication in any form.

Indeed, Ugandan laws vests the government with wider powers to conduct interception to communication without much guarantee of safeguarding and respect to human rights such as the right to privacy. This is stressed and reiterated in a report of periodical review submitted to the United Nations accusing the *Regulation of Interception of Communication Act* that it has given far-reaching powers to intercept communication of individuals, groups or organisations, while respect and safeguard for human rights is abandoned.[3]

5.3.4.1 Legality and Justifications

The *Regulation of Interception of Communication Act* provides for procedures and justifications for interception of any form of communication. This law is a base for legality of interception in cyber laws in Uganda. The law points categorically officers who may apply for a warrant of interception to a designated judge.[4] These officers include; (a) the Chief of Defence Forces or his or her nominee; (b) the Director General of the External Security Organisation or his or her nominee; (c) the Director General of the Internal Security Organisation or his or her nominee; or (d) the Inspector General of Police or his or her nominee.[5] The law requires further specific information to be given to a Judge issuing a warrant.[6] The designated Judge upon satisfactions of the justifications given under the law may issue a warrant. The justifications sought under the law are worth quoting hereunder *verbatim*:

> *"(1) A warrant shall be issued by a designated judge to an authorized person referred to in section 4(1) if there are reasonable grounds for a designated judge to believe that—*
>
> *(a) an offence which may result to loss of life or threat to life has been or is being or will probably be committed;*
>
> *(b) an offence of drug trafficking or human trafficking has been or is being or will probably be committed;*
>
> *(c) the gathering of information concerning an actual threat to national security or to any national economic interest is necessary;*
>
> *(d) the gathering of information concerning a potential threat to public safety, national security or any national economic interest is necessary; or*
>
> *(e) there is a threat to the national interest involving the State's international relations or obligations."*[7]

Moreover, the application sought by an authorised person must reach the issuing Judge within forty eight hours for determination.[8] The scope and extent of interception is also covered under the law. It provides validity of a warrant to be three months subject to renewal for good cause; it should specify the name and the address of the interception subject and the manner of interception; places strictly cooperation to communication services providers; specifies the apparatus and means to be used in interception; and provides for any other details necessary for the interception.[9]

5.3.5 Observations under Ugandan Laws

Though at glance, the Ugandan laws seem to have conferred the government with wider powers to conduct interception against any form of communication of an individual, group or organisation; the law regulating interception contains provision which gives power to the designated Judge in his or her opinion or if the circumstances requires to rejecting order for issuance of interception warrant; or to amend or revoke the issued warrant.[10] These guarantees defence by the defendant and control on the other hand by the court in ensuring criminal justice.

Despite of the fact that the Ugandan government is blamed for violating human rights in the course of its implementation in regulating information communication and technologies, the government in response to the blames raised, argues by justifying that the government among others, desires to 'keep morals', national security and the fight against terrorism.[11] In fact, the justifications sought by the government are pertinent to note for the well-being of the country in as much as human rights such as the right to privacy.

5.0 Conclusion

After exploring and analysing the cyber laws of the three East African Countries namely; Tanzania, Kenya and Uganda, now I venture and display the findings. It is undisputable fact that, the right to interception under cyberspace is a global challenging issue. Its legality and justifications should be laid down under the cyber law(s) in existence of a particular country. The profound basic right to privacy of an individual as it is enshrined in the international, regional and national instruments should be honoured not only under traditional laws but cyber laws as well. However, in case of any justifiable reasons for interception of communication of an individual, group or organisation, it should be shown that it is legally provided and its justification should be measured in the parameters of two variables, that is, public interests and private interests.

On the other hand, the striking balance between the two variables should not outpace the national interest nor detrimental to the individual's right to privacy for the State is responsible to ensure that both human rights and national security are safeguarded. Thus, in certain circumstances the State can legally enjoy a right to intercept at the expense of right to privacy of an individual. However, it should be born in our mind that the right to privacy is not an absolute right.[12] The right to privacy is subject to some limitations and purposes which are intended to serve.[13] Conversely, if interception is conducted illegally and without justifications thereof, then such interception is bad in law. When the interception is measured within the parameters of limitation purposes and fails to meet the standards set out, the resultant effect is violation of human rights casted to an individual.

It is discovered further that the provisions vary from one law to another within a country; and from one country to another.[14] Legality and justification of interception under the laws are of vital importance. It should be kept in our mind that, it is lucrative and common principle that criminal laws contain two parts, that is, substantive and procedural law. Judicial warrants for interception is meant for interpose a neutral and detached magistrate and the right of citizens as observed in *People v Bialostok (supra)*.

Therefore, it follows that absence or unclear or conflicting procedures regarding interception of communication cause maladministration of justice in practice, hence violation of human rights - the right to privacy. In addressing this

1 The Ugandan Regulation of Interception of Communications Act, 2010
2 S. 3 *Ibid*
3 The Republic of Uganda, "ARTICLE 19's Submission to the UN Universal Periodic Review," *Submitted for consideration at the twelfth session of the UPR Working Group,* October 2011, at p.2
4 S. 4(2) of the Regulation of Interception of Communication Act, 2010
5 S. 4 (1), *Ibid*
6 S. 4 (3), *Ibid*
7 S. 5 (1), *Ibid*
8 S. 5 (2), *Ibid*
9 S. 6, *Ibid*
10 S. 5 (3), *Ibid*
11 Mayambala, R. K. "Examining the Nexus Between ICTs and Human Rights in Uganda: A Survey Of The Key Issues," *A Presentation Paper Prepared for the International Workshop on the Nexus Between ICT and Human Rights, organised by Human Rights and Peace Center, Faculty of Law, University of Makerere, Uganda with support from the International Development Research Centre, Ottawa, Canada*, 2nd to 4th April, 2009, at p. 4.
12 *Norris v Attorney General* (1984) I.R 587
13 *Campbell v MGN Ltd* (2004) 2 AC 457
14 Tanzania, Kenya and Uganda respectively

point, it is my firm submission that, though justifications given by the government of Uganda, overlaps the human rights which are protected; insecurity of the nation is more damaging than the sufferance sustained by the victim for violating his right to privacy. Therefore, it is acceptable that interception should be justified at the detriment of the victim. However, in so doing, a striking balance between national security and individual's right to privacy must be accorded in accordance with proper laid interception procedures.

As opposed to Ugandan cyber laws, the Kenyan and Tanzanian cyber laws analysed above, places enormous interception mandate directly to the State authorities. The vested powers threaten the individual's right to privacy despite the fact that it is subjective one. Judicial approval regarding interception order of individual's communication is, and in fact a paramount concern as it touches basic human rights of an individual. However, the new cyber law in Kenya has introduced a provision on prevention and control of misuse of exercising power given under the law by the police officer or authorized person. The fact that interception is allowed under the law, then absence of the proper interception procedures is defeated by the cardinal principle of rule of law that the law must be fair and accommodates respect for human rights.