IN THE HIGH COURT OF TANZANIA

(MAIN REGISTRY)

AT DAR ES SALAAM

MISCELLANEOUS CIVIL CAUSE NO 9 OF 2016

(CORAM: KOROSSO, KITUSI & ARUFANI, JJJ)

JAMII MEDIA COMPANY LTD.....PETITIONER

VERSUS

THE ATTORNEY GENERAL.....1ST RESPONDENT

INSPECTOR GENERAL OF POLICE.....2ND RESPONDENT

DATE OF LAST ORDER.....2/12/2016

DATE OF JUDGMENT.....8/3/2017

I.P.KITUSI, J

JUDGMENT

This is a petition under Articles 26(2) and 30(3) of The Constitution of the United Republic of Tanzania, Section 4 of the Basic Rights and Duties Enforcement Act, Cap 3 and Rule 4 of the Basic Rights and Duties Enforcement (Practice and Procedure) Rules 2014. Jamii Media Company Ltd, the petitioner, moves the court to declare that the provisions of Sections 32 and 38 of the Cybercrime Act No 14 of 2015 are unconstitutional for offending the provisions of Article 13(6) (a), 16 and 18(1) & (2) of the Constitution of the United Republic of Tanzania,

1977 as amended. We shall hereafter refer to the Constitution of the United Republic of Tanzania, 1977 as the Constitution, and to the Cybercrimes Act No 14 of 2015 as the Act. The Basic Rights and Duties Enforcement Act, Cap 3 shall simply be referred to as Cap 3, while the Basic Rights and Duties Enforcement (Practice and Procedure) Rules, 2014 shall be called the Rules.

In terms of Rule 13 of the Basic Rights and Duties (Practice and Procedure) Rules, 2014 this petition was argued by way of written submissions and later brief oral presentations were made by Mr Benedict Alex, learned advocate for the petitioner, and Mr Richard Kilanga, learned Senior State attorney, for the respondents. To a very great deal, we are indebted to them for their research and assistance in this case which involves an area that is admittedly new. We shall refer to their inputs whenever it is necessary, but we consider all inputs to be of very great value, even those which, for some reason, we may not refer to.

We find it relevant to expound the fact that the Cybercrimes Act was enacted by Parliament in 2015, and it came into force on 1st of September 2015, through Government Notice No 328 of 2015.

The background to this petition as told in the pleadings is to the following effect; the petitioner owns and operates a website registered as Jamii Forums and Fikra Pevu, in which subscribers or users are permitted to post, engage and participate in discussion of issues involving various subjects. The issues may be of social, economic or political relevance in the society. It is the petitioner's policy that users of the website may access it without identifying themselves, a policy

known as Anonymity, which, according to the said petitioner, promotes the right to privacy.

It is contended that since the commencement of the Act, the police, especially the Cybercrimes Unit of the Police Force, have been issuing a number of orders to the petitioner demanding it to disclose information relating to its customers or subscribers. These orders, in this ruling to be called "disclosure orders", were being and are being made under Section 32 of the Act. Specific instances of disclosure orders are; on 16th January,2016 the Criminal and Investigation Department (CID) branch of the Tanzania Police Force issued the petitioners with a letter demanding disclosure of a user whose identity was IP, and who had posted information saying that; "Mengi ajitoa rasmi kwa Lowassa".

On 26th January, 2016 the Cybercrimes Unit of the Tanzania Police Force issued the Petitioner with another letter of demand, this time requiring disclosure of a user who had posted information saying; "Charles Kimei (CRDB) jiuzulu, Kashfa ya Kontena, tiketi TFF, wanafunzi na ujambazi CRDB" and also; "Wizi wa Bank ya CRDB part II"

The petitioner's written response to the disclosure orders was that the Police also disclose to it the nature of criminal investigations which they were conducting, so as to justify the submission of the information demanded. The petitioner states that they reacted in that way because they have a dual duty; the first duty being towards the customers or users of the website whose privacy must be protected. The second is the duty towards law enforcement agents with whom they must cooperate on issues of national security. It is stated further that despite the petitioner's good intentions, the Police are bent in their threat to

prosecute. This is because on 4th February, 2016, they threatened to prosecute them under Section 22 of the Act, although on 23rd of February 2016 the Police issued the Petitioners with yet another letter of demand. The petitioner therefore decided to file this petition to challenge the Constitutionality of Sections 32 and 38 of the Act.

The petition is based on the following legal grounds, according to the submissions by the learned advocate representing the petitioner. That Article 16 (1) of the Constitution provides for the right to privacy, but Section 32 of the Act takes it away or interferes with it. Secondly that Article 13 (6) (a) of the Constitution provides for the right to be heard but Section 38 of the Act empowers the police to condemn the service providers unheard including taking away their electronic devices without hearing them. Article 16 (1) of the Constitution provides;

> *"16.-(1) Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and* ***private communications.***"

To begin with we have to decide on what are the issues for determination in this petition, because the parties are not at one on this. Counsel for the petitioner has invited us to consider the following issues;

1. Whether the provision of Section 32 of the Act infringes the right to privacy as provided for under the Constitution.

2. Whether the provision of Section 32 of the Act restricts the right to freedom of expression as provided under Article 18 of the Constitution.

3. Whether the provision of Section 38 of the Act which restricts appearance of a person against whom an application is made to defend himself before court of law infringes the right to be heard as provided for under the Constitution.

On the other hand the learned Senior State Attorney has proposed the following issues;

1. Does the High Court have the mandate/powers/jurisdiction to prevent the police to carry on the investigation under the Basic Rights and Duties Enforcement Act Cap3 R.E 2002.

2. Does the High Court have the jurisdiction under Basic Rights and Duties Enforcement Act Cap3 R.E 2002 to compel the Police to disclose the offences committed or suspected to have been committed by those users.

3. Whether the petitioner have complied with his duty under Section 39 (4) (c) of the Cyber Crime Act.

Without wasting time and with respect, we disagree with the learned Senior State Attorney's suggested theme of issues. Not only are the issues proposed by him novel to the pleadings as rightly submitted by the Petitioner's advocate in his rejoinder, but they are framed in a way that suggests that once powers are conferred on a body by statute, the court has no power to question their legality. We think we cannot go along with the learned Senior State Attorney on that, and we seize this opportunity to remind the learned Senior State Attorney and others that nobody is above the law. The six principles laid down by Samatta, JK (as he then was) in the case of **Mwalimu Paul John Mhozya V. The**

Attorney General (N0. 1) [1996] TLR 130 were as relevant in that case as they are in this, because it involves a conflict between individual rights against state power. The police, just as anyone else, are not above the law. We are also inspired by a decision of the Supreme Court of Uganda in the case of **Ssemwogerere and others V. Attorney General** [2004] 2 EA where the court held that it was an abdication of duty for the Constitutional Court to deny that it had jurisdiction to declare an Act of Parliament unconstitutional.

We hope we have sufficiently demonstrated that the main bone of the contention is the validity of the impugned provisions of Sections 32 and 38 of the Act. On that basis we are satisfied that the following issues will address the competing views of the parties;

1. Whether the impugned provisions of Sections 32 and 38 of the Act are constitutionally valid

2. If not what are the consequences

3. To what reliefs are the parties entitled

The petitioner is challenging infringement of the right to private communications upon issuance of disclosure orders by the respondents, and that victims of such police action under Section 38 are inadvertently condemned unheard. Counsel for the petitioner expounded on the right to privacy as meaning, the right to maintain a domain and the ability to choose which part of it to share with others and which part not to, arguing that the right to privacy is the essence of the petitioner's Policy of Anonymity. Later it is submitted that in recognition of the right to privacy the Canadian Supreme Court held in the case of **R. V.**

Spencer [2014] SCC 43, that anonymity is one of the three concepts of privacy.

> *"...the identity of a person linked to their use of internet must be recognized as giving rise to privacy interest beyond that inherent to the person's name, address and telephone number found in the subscriber information."*.

The petitioner's counsel alluded to the fact that they appreciate the fact that there are always limitations to human rights and that the law allows for some interferences. Article 16 (2) provides for instances of interference to the right to privacy. Article 16 (2) reads as under;

> *"(2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article".*

The petitioner went on to submit that Section 32 (1) of the Act is a result of Article 16 (2) of the Constitution. This provision, he contended encroaches upon the right to private communications by empowering the police to issue disclosure orders.

The petitioner's main point of contention is that in order for an encroaching provision to be valid it must not only be saved by Article 30 (1) and (2) of the Constitution, but it should also pass the two tests developed in the cases of **DPP Versus Daudi Pete** [1993] 22 and **Kukutia Ole Pumbun and Another Versus Attorney General and**

Another [1993] TLR 159. It is now settled principle that there are two tests that can validate derogation of provision of the law and they are; (i) the law should not be arbitrary and; (ii) it should not be too wide as to go beyond what is intended to be achieved.

We think at this juncture we need to state that the two factors that were developed in **Daudi Pete** and **Kukutia Ole Pumbun,** have since then become litmus papers for testing the validity of provisions that seek to encroach upon human rights. We do state this at this point so as to narrow the scope of our decision, and limit it to testing the challenged provisions against these two factors. We find it relevant to therefore proceed to examine submissions by the learned advocate for the petitioner on the two important factors, after which we shall refer to submissions by the respondent's Senior State Attorney.

On the first test, that is arbitrariness, Mr Alex for the petitioner submitted that Section 32 is arbitrary because it does not provide for the procedure to be followed by the police in issuing the disclosure orders. The petitioner's complaint is that the said provision of Section 32 of the Act does not require the police to state the criminal case which may necessitate issuance of disclosure orders. The learned advocate went on to submit that there are no Regulations made by the Minister responsible for communication as required by Section 39 of that Act. That since Article 16 (2) of the Constitution requires state authority to put in place procedures governing the circumstances and manner of interfering with the basic rights stipulated, and as the Regulations are not yet in place, then the provision of Section 32 (1) of the Act is arbitrary for violating that constitutional requirement. When asked by the court whether his position would remain the same if the Minister

responsible made the requisite Regulations, Mr Alex submitted that he would not change, because this complaint regarding absence of Regulations is an alternative to another complaint. What then is the other complaint?

The contention is that Section 32 of the Act is too wide because, sub section (4) thereof requires a person to surrender to the police, information in a form that can be taken away. Making reference to electronic devices such as laptops, mobile phones, IPads, tablets, etc, the learned counsel submitted that if an investigator takes away one such device in order to access one piece of information relevant to a particular investigation, there is no guarantee that by taking the same the investigator will not access other pieces of information contained in the same device and irrelevant to the matter being investigated.

Mr Alex cross referred to Section 38 of The Criminal Procedure Act which relates to search and that unlike Section 32 (4) of the Act which also deals with search, the former provision has many safeguards. The learned counsel asserted that Section 32 (4) is unreasonable, arbitrary and lacks safeguards against possible abuse by the police, and for that it violates Article 16 (1) and (2) of the Constitution.

When considering the petitioners submissions on the issue at hand it is important to understand that we are not losing sight of the fact that the petition is based on mainly two grounds; one is that the provision of Section 32 of the Act violates against the constitutional right to privacy enshrined under Article 16 (1) of the Constitution; two is that if this right has to be encroached upon to achieve any of the objectives under Article 30 (1) and (2) of the Constitution the law purporting to do that

must meet the two tests in the cases of **Daudi Pete** and **Kukutia Ole Pumbun(supra).**

On the respondents' side, they opposed the petition and maintained that Section 32 of the Act is constitutional. The learned Senior State Attorney started with presentation of a brief background to the enactment of the Cybercrime Act. He stated that technological advancement has brought with it many legal and operational challenges, and that the police who have a statutory duty to maintain law and order would not be able to cope with the rapid and emerging ways of commission of crimes associated with the digital world if the legal challenges had not been addressed. The Cybercrime Act was therefore enacted with the good intention to protect the victims of cybercrime and to get the guilty arrested and prosecuted. He stressed the fact that Section 32 (1) of the Act empowers the police to issue disclosure orders for purposes of investigation and/or prosecution of offences. The respondents do not deny the fact that the police issued the disclosure orders referred to in the petition, but it was their assertion that the issuance was justified.

There are two grounds relied upon by the respondents, in our view. The first is that Section 32 (1) has been lawfully enacted, therefore the legislation is lawful. Secondly it is argued that the provisions being challenged are merely investigatory and do not determine the rights of the people conclusively. Some provisions including Section 5 of the Police Force and Auxiliary Services Act, Cap 322 and those under the Criminal Procedure Act, Cap 20 which deal with investigation, have been cited to show their similarities with provisions also dealing with investigation, under the Act. Further it is submitted

that disclosure orders made by the police under Section 32 (1) of the Act do not infringe upon Article 16 of the constitution, because they are intended to obtain the names of people who have published information that may turn out to be relevant to some offences under investigation. The learned Senior State Attorney further submitted that the Act does not require the police to disclose to the recipient of the disclosure orders, the offences under investigation as submitted by the petitioners.

On the safeguards, it has been submitted by the respondents that Section 36 of the Act provides for an opportunity to resort to court by making applications where disclosure cannot be made voluntarily. It is their contention that section 32 (1) of the Act is not too wide because the disclosure orders being complained of may only be issued by police officers who are senior in rank.

It is also submitted in relation to the petitioner's Privacy Policy referred to, that such privacy policy cannot override the law. On the constitutional right to privacy, the learned Senior State Attorney submitted that the right to privacy cannot override public interest. He cited the case of **Julius Ndyanabo Versus the Attorney General** [2004] TLR 14 for the principle that there is always a need of balancing between individual rights and public interest. It is submitted in addition that the disclosure orders were all for investigations purposes in line with the law.

As for the two tests for validation of legislation, the learned Senior State Attorney submitted that Section 32 of the Act is valid and has been saved by Article 30 (1) of the Constitution. First on the contention that Section 32 is wide and thus arbitrary the submission is that it is not, by

reason that the disclosure orders were specific, not wide as contended. On the contention that the provision of section 32 is unreasonable the learned Senior State Attorney stated that it is not, for the reason that the disclosure orders are issued only during investigations.

The respondents counsel referred to Article 29 (5) of the Constitution and a number of cases to bring home the fact that human rights are not absolute rights to be enjoyed by an individual in total disregard of the rights of others in the society. Article 29 (5) of the Constitution provides;

> *"(5) In order that all persons may benefit from the rights and freedoms guaranteed by this Constitution, every person has the duty to so conduct himself and his affairs in the manner that does not infringe upon the rights and freedoms of others or the public interest."*

Then, the learned Senior State Attorney repeated his reference to the case of **Julius Ndyanabo** (supra) for the principle that the Constitution strikes a balance between the rights of an individual and social control. He also referred to the case of **Shreya Singhai V. Union of India** (2009) cited by the petitioner and drew the Court's attention to a paragraph where the court stated;

> *" In the U.S, if there is a compelling necessity to achieve an important governmental or societal goal, a law abridging freedom of speech may pass muster."*

The learned Senior State Attorney distinguished the cases cited by the learned counsel for the petitioner, these are; the case of **Mcintyre V.**

Ohio Elections Commission (1995); **Transport Equipment Ltd, and John Nolan V. Devram P. Valambia**, Civil Application No. 49 of 1993 and; **R V. Hoho [2009] 1 All SA 103 SCA.** Reproducing the relevant facts in the latter case which involved criminal defamation, he quoted the following paragraphs to show that the case is not of any assistance to the petitioner.

> *" But the freedom of expression is not unlimited" (page 29)*
>
> *" Protection of reputation is conducive to the public good. It is in the public interest that the reputation of public figures should not be debased falsely."* (Page 30)

Even the Article cited by the petitioner from the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, has been quoted by the learned Senior State Attorney to hit back on the very petitioner. It says that the right to privacy can be subject to restrictions or limitations for the aims of administration of justice, prevention of crime or combating terrorism.

It is therefore submitted that the Act is a creature of Article 30 (1) and (2) of the Constitution, which gives the State powers to enact laws for actualizing the human right. Mr Kilanga Learned Senior State Attorney submitted that the intention behind the enactment of the Act is to facilitate investigation of crime, collection of electronic evidence, and use of that evidence in court. That Section 32 (1) of the Act which gives the police powers to issue disclosure orders for purposes of criminal investigation and prosecution is not arbitrary and cannot be unconstitutional.

As shown in the preceding pages of this ruling, during the counsel's brief oral submissions before us, and while taking note of Section 33 (2) of the Act which empowers the Minister responsible for Communication to make Regulations, we wanted the views of Mr Alex and Mr Kilanga on whether the position of the petitioner would be different if the Regulations were in place. We have already referred to the response of Mr Alex for the petitioner. On his part Mr Kilanga, learned Senior State Attorney, submitted that this petition is not the right procedure for challenging the Minister's inaction. He submitted that the petitioner should have filed an application for Judicial Review for orders of mandamus. The learned Senior State Attorney invited us to bear the following principles in mind when dealing with this matter;

1. That Section 5 of the Police Force and Auxiliary Services Act [Cap 322 R.E 2002] and; Part I of the Criminal Procedure Act Cap 20 give the police the duty to prevent and detect crimes and also to search and seize.

2. Human rights are not absolute and to treat them as so is to invite anarchy in the society.

3. Constitution is a living document which should be interpreted by considering changes in the society as well as technological development

4. A legislation is presumed legal until the contrary is proved

5. The Act should not be read in isolation. It should be read together with provisions of other laws such as the Interpretation of laws Act Cap 1, the Penal Code Cap 16, the

Criminal Procedure Act Cap 20, the Police Force Act, Cap 322, The National Security Act etc.

6. The public interest prevails over individual interests as provided under Article 30 (2) of the Constitution

7. Standard of proof in constitutional petition is beyond reasonable doubt.

We wish to make one point clear, that in discussing the two tests, the focus is on the provisions of Section 32 and 38 of the Act not on the actions by the police. We have decided to say so at this point because we are afraid that we have discerned that in the midst of presentation of arguments on some points the submissions have tended to address the propriety of the actions taken rather than the law under which they are purportedly done. For instance the submission by the learned Senior State Attorney that Section 32 is not too wide for the reason that the disclosure orders were specific, tends to miss the point that it is the law that is alleged to be too wide. Thus we shall keep an eye on it lest it is overstepped. Similarly the submission that all disclosure orders were made for investigation purpose, it misses the point raised by the petitioner that because of absence of Regulations, there is no guarantee against misuse of the powers by the police to investigate crimes.

After going through the rival arguments by the learned attorneys for both sides we are satisfied that the genesis of this petition is a complaint that some acts that have been done by the Police have been so done under a piece of legislation which does not meet the constitutional validity tests provided for under Article 16 (1) of the Constitution. We consider it appropriate to commence by appreciating

the background to the enactment of the Cybercrime Act, and that it is a result of a new direction caused by developments in the world of Information Communication and Technology. We associate ourselves with the observations made by Adam Mambi in his book titled, ICT LAW BOOK, Mkuki na Nyota Publishers Ltd, 2nd edition, 2014, where the learned author made the following observation;

> *" Most crimes in Tanzania are regulated by laws such as the Criminal Procedure Act, the Penal Code, the Extradition Act and other related laws. However most of these laws are out of date and do not take into account the development of technology that is always changing very rapidly. These might hinder the development of e-commerce as some of the new offences are not addressed."*

It can be concluded therefore that the enactment of the Act was, as submitted by the learned Senior State Attorney, necessary in order to respond to the gaps that had emerged in the existing laws. This intention was expressed in the presentation of the Cybercrime Bill as recorded in the Hansard, and quoted in the case of **Jebra Kambole V. The Attorney General,** Miscellaneous Civil Cause No 32 of 2015, HC (unreported).

We agree with the learned Senior State Attorney again, and this is common ground, that in disposing of this petition we should be guided by the following matters or principles. One is that an Act of parliament is deemed to be constitutional until it is proved otherwise. Secondly the right to privacy is a constitutionally guaranteed right under Article 16 (1) of the Constitution, and that the right to private communication is a

component of that right. Thirdly, however legitimate was the intention for enacting the Act under scrutiny, the derogative provisions have to be validated by the two tests. Our duty is to balance between individual human rights on the one hand and public interest on the other.

We are aware of the Minister's duty to make Regulations under Section 39 (2) and 51 of the Act, and that he has not made them. We have referred to the response of Mr Alex, learned advocate, on our hypothetical question regarding what would be his position if the Minister had made the Regulations under the Act. We are nevertheless asking ourselves whether the provisions of Sections 32 and 38 would be held to be arbitrary for the reason that the Regulations envisaged in that law are not yet in place. Here we remind ourselves of the principle, mentioned but a while ago, that the provisions of Sections 32 and 38 of the Act are presumed constitutional until proved otherwise. We understand that since the petitioner is the one who alleges that those provisions are unconstitutional, the burden is in him under Section 110 of the Evidence Act, [Cap 6 RE 2002] to prove that they are. With respect, we think a piece of legislation is arbitrary if it has not been lawfully enacted, that is, if it is not a result of the legislative powers of parliament, or although passed through legislative process, it does not appeal to reason. The word 'arbitrary' is defined in Black's Law Dictionary, page 119, as;

> *" 1. Depending on individual discretion... determined by a judge rather than by fixed rules, or law.2. Founded on prejudice or preference rather than on reason or fact".*

We are satisfied that the reference to "rules or law" in the above definition does not include a situation as the present, where the law is there and makes mention of regulations or rules, but they are yet to be in place. We note that invariably all statutes that provide for making of Regulations by the Ministers responsible, it takes a while before the said regulations are formulated. We have examined a few legislations in order to satisfy ourselves if they have their requisite Regulations ready and when. These are the Executive Agencies Act, Cap 245, the Social Security (Regulatory Authority) Act, Cap 135 and the Office of the Attorney General (Discharge of Duties) Act, 2005.

It should be understood that we are not justifying a wrong by a another wrong, but we are satisfied that Regulations compliment the law, as it was held by James, L.J in the case of *A.G V. Keyser's Royal Hotel* [1920] A.C 551 cited in the case of **Julius Ndyanabo (**supra). Reasoning along that line, we are satisfied that regulations will complement the law better when the law has become operational. We are inclined to agree with the learned Senior State Attorney that if action had to be taken in respect to absence of Regulations in this case, then it would be to apply for judicial review.

The other reason advanced by the petitioner for challenging the impugned provisions is that they do not provide for safeguards against possible abuse by the police. One possible abuse has been cited, that is the possibility of over access to information where a device containing various information is taken away by the police who are in need of only one type of information. The learned Senior State Attorney responded by submitting that the fact that the orders may only be made by senior

police officers and there is an option to resort to court in the event one is not willing to release the data, are enough safeguards.

With respect, we think that it is only by reading the impugned provisions that one can tell if they are arbitrary and not proportional as alleged. The provision of Section 32 of the Act states;

> *'32-(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer in charge of a police station or law enforcement officer of a similar rank may issue an order to any person in possession of such data compelling him to disclose such data.*
>
> *(2) The order issued under subsection (1) shall be granted to a law enforcement officer who shall serve the order to the person in possession of the data.*
>
> *(3) Where the disclosure of data cannot be done under subsection (1), the law enforcement officer may apply to the court for an order compelling;*
>
> *(a) A person to submit specified data that is in that person's possession or control; or*
>
> *(b) A service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.*
>
> *(4) Where any material to which an investigation relates consists of data stored in a computer system or device, the request* ***shall be deemed to require the person to produce or give access***

to it in a form in which it is legible and can be taken away."

After closely reading Subsection (4) of Section 32 of the Act, we do not see the essence of the petitioner's worry, because in our interpretation of that section, it does not empower the police to take away the devices as contended. The words *"shall be deemed to require the person to produce or give access to it in a form in which it is legible and can be taken away"* under that subsection of the Act are in reference to data not to the device. Our understanding of that section is that the person, to whom the request has been made, like the petitioner in this case, may print the information such that it can be read and/ or taken away by the investigators in a printed form. But there is another safeguard in our view, and we respectfully agree with the learned Senior State Attorney again, in that if disclosure of information is not done voluntarily, then subsection 3 of section 32 and Section 36 of the Act provide for an option to seek court intervention.

On the contention that section 32 is unreasonable, we wish to start by stating that there is no standard for measuring reasonableness of a statute as it was stated in the case of **Julius Ishengoma. (supra).** In our view this is where our duty of balancing the interests of an individual against those of the public comes to play. In playing that role we can only adopt the words of Patanjali Sastri, CJ, also reproduced by the learned Senior State Attorney, in *State of Madras V. V.G. Row* [1952] SCR 597 quoted in **Julius Ishengoma**;

> *" The test of reasonableness should be applied to each individual statute impugned, and no abstract standard, or general pattern of*

reasonableness can be laid down as applicable to all cases. The nature of the right alleged to have been infringed, the underlying purpose of the restrictions imposed, the extent and urgency of the evil sought to be remedied thereby, the disproportion of the imposition, the prevailing conditions at the time should all enter into the judicial verdict."

We shall therefore measure the reasonableness of Section 32 by applying the principles above quoted.

The petitioner submitted that privacy in the internet communication is very central considering the nature of the communication that goes through that medium. It was further submitted that Section 32 is unreasonable and arbitrary for lack of safeguards against abuse or misuse of the powers.

The fact that these powers are exercised without giving the victims a hearing is supported by the cases of **Wiseman and Another V. Borneman and Others,** [1969] 71 ITR 651 Cal; **The Hon A.G and Another V. Munuo Ng'uni** [2002] TLR .

In response to this, the respondents submitted that the cases cited by the petitioner to justify his point were irrelevant to this case which deals with computer data which may be destroyed, deleted, altered or tempered with within a short time.

In testing the reasonableness of Section 32, we have decided to borrow from Adam Mambi again where the learned author shows some security issues that emerge with technological advancement. The learned author has written the following at page 127 -128;

'There are legal issues which affect the development of electronic financial services in Tanzania. There is no highly assured security against fraud and other related cyber offences given lack of legal framework that regulate this area in Tanzania".

We have earlier stated that the Act came to address these gaps. We are asking ourselves whether the Act is unreasonable in requiring the people in possession of relevant data to disclose them to the investigators under the circumstances. When we balance the petitioner's interests in this case against the wider interests of the public we are satisfied that the ground to support this petition is thin.

It is clear to us that the restriction to the right to hold information is not peculiar to Tanzania. We have read Article 19 (2) and (3) of the International Covenant on Civil and Political Rights, which provides;

" (2) Everyone shall have the right to freedom of expression; the right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

(3). The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary;

(a) For respect of the rights or reputation of others;

(b) For the protection of national security or public order, or of public health or morals."

We have reached a conclusion that Section 32 of the Act is within the proportional restrictions permissible not only in our jurisprudence but also internationally. We hold the contention in respect of Section 32 of the Act to be baseless and we dismiss it.

We turn to the complaints in respect to Section 38 of the Act. The said provision reads;

> *" 38. The proceedings for hearing of an application under this part shall be ex parte and in camera."*

We think this issue need not take long. The application referred to under this section is the application under Section 36 of the Act made by the police when one refuses to disclose information voluntarily. This is the denial of a hearing that the petitioner challenges under Article 13 (6) (a) of the Constitution. The learned Senior State Attorney has submitted that these are investigation stages.

With respect we do not agree with Mr Alex that the ex parte hearing at this stage amounts to a denial to a hearing. We have deemed it necessary to compare Section 38 of the act with Section 51 of the Criminal Procedure act, cap 20. Under the latter provision, a police officer interrogating a suspect and recording his statement needs to seek extension of time from a police officer in charge of a station if the statutory time runs out. The provisions of Section 38 cannot, in our view be said to be a denial of the right to be heard while it is at a stage when the rights are not conclusively determined. Even then, we think the involvement of a court is a safeguard against abuse by the police.

It is our conclusion and for the reasons stated herein, that the petitioner has failed to prove the claims before the court that the provisions of Sections 32 and 38 of the Cybercrime Act, 2015, are unconstitutional. The petition is therefore dismissed and we find no plausible reasons to order for costs under the circumstances.

Dated at Dar es Salaam this 8th day of March, 2017.

.....
W.B. KOROSSO
JUDGE

.....
I.P. KITUSI
JUDGE

.....
I. ARUFANI
JUDGE