**REPUBLIC OF KENYA**

**IN THE HIGH COURT OF KENYA AT MILIMANI (NAIROBI)**

**CONSTITUTIONAL & HUMAN RIGHTS DIVISION**

**PETITION NO.206 OF 2019**

**AND**

**IN THE MATTER OF THE ARTICLE 2, 3,20,22,23,116,165,258 & 259 OF THE CONSTITUTION OF KENYA**

**AND**

**IN THE MATTER OF THE ALLEGED CONTRAVENTION OF HE RIGHTS AND FUNDAMENTAL FREEDOMS UNDER ARTICLES 19,21,24,25,27,28,31,33,34,35,40 & 50 OF THE CONSTITUTION OF KENYA**

**AND**

**IN THE MATTER OF THE ALLEGED CONTRAVENTION OF ARTICLES 1, 10,118 & 238 OF THE CONSTITUTION OF K ENYA, 2010**

**AND**

**IN THE MATTER OF SECTION 3,5,16,17,22,23,24,27,28,29,31,32,33,34,35,36,37,38,39,40,41,48,49,50,51,52 & 53 OF THE COMPUTER MISUSE AN CYBERCRIMES ACT**

**AND**

**IN THE MATTER OF STANDING ORDERS 119,127,130,131 & 133 OF THE NATIONAL ASSEMBLY STANDING ORDERS**

**BETWEEN**

**THE BLOGGERS ASSOCIATION OF KENYA (BAKE)..... PETITIONER**

**VERSUS**

**THE HONOURABLE ATTORNEY GENERAL.....1ST RESPONDENT**

**THE SPEAKER, NATIONAL ASSEMBLY.....2ND RESPONDENT**

**THE INSPECTOR GENERAL OF THE NATIONAL POLICE SERVICE.....3RD RESPONDENT**

**THE DIRECTOR OF PUBLIC PROSECUTIONS.....4TH RESPONDENT**

**ARTICLE 19 EAST AFRICA.....1ST INTERESTED PARTY**
**KENYA UNION OF JOUNALIST.....2ND INTERESTED PARTY**

# JUDGMENT

## Petitioner's Case

**1.** The computer misuse and Cybercrime Act 2018 *(hereinafter referred to as the "Act")* was assented to a law on 16th May 2018 having been considered and passed by the National Assembly on various dates between October 2017 and April 2018. The Act is an Act of parliament to provide for offences relating to computer systems; to enable timely and effective detection; prohibition, prevention, response; investigation and prosecution of computer and cybercrimes to facilitate international co-operation in dealing with computer and cybercrimes matters; and for connected purposes.

**2.** The petitioner through a petition dated 29th May 2018 seeks the following orders:-

a) That this application be certified urgent and be heard *ex parte* in the first instance;

b) That pending the hearing and determination of this application *inter partes,* a conservatory order does issue suspending the coming into force of the Computer Misuse and Cybercrimes Act, 2018 and in particular the coming into force of Sections 5,16,17,22,23,24,27,28,29,31,32,33,34,35,36,37,38, 39,40,41,48,49,50,51,52 & 53 of the Computer Misuse and Cybercrimes Act, 2018.

c) That pending the hearing and determination of the Petition, a conservatory order does issue staying the coming into force of the Computer Misuse and Cybercrimes Act, 2018 and in particular to stay the coming into force of Sections 5,16,17,22,23,24,27,28,29,31,32,33,34,35,36,37,38, 39,40,41,48,49,50,52 & 53.

d) That costs of the application be provided for.

**3.** The petitioner further contends that the requirement of public participation was not satisfactorily met during the consideration of the Bill and that standing orders 130, 131 and 133 of the National Assembly standing orders are inconsistent with the constitution in so far as they allow the inclusion of clauses to a bill without public participation.

**The 1st and 3rd Respondent's Case**

**4.** The first and 3rd Respondents are opposed to the petition. The 1st Respondent filed a Replying affidavit sworn by the Deputy Solicitor General; Christine Agimba on 20th June 2018, in response to petitioner's petition. The 3rd Respondent similarly filed a Replying affidavit sworn by the Inspector General, National Police Service, Joseph

Kipchireir Boinnet, **MGH,** nic **(AU)** sworn on 20th June 2018 in response to the petitioner's petition.

**5.** It is 1st and 3rd Respondents contention that in determining the merit or otherwise of this petition the court should seek guidance from the following legal principles: - the doctrine of separation of powers; the state duty of care to its citizenry; presumption of constitutionality of statute; Limitation of rights in balancing private and public interest.

**The 2nd Respondent's Case**

**6.** The 2nd Respondent is opposed to the petition. It relies on a Replying affidavit by Michael Sialai sworn on 21st September 2018. It is the 2nd respondent's case that the alleged dispute is based on perceived grievances which are likely to arise should the membership of the National computer and cybercrimes coordination committee established under section 4 of the Act be of the same gender. It is contended that this is not a basis for filing a petition, as it is purely hypothetical conjectural and speculative. It is further 2nd respondent's case that in the absence of a dispute, the petitioners lacks status, and can at best be described as busy bodies.

## The 4th Respondent's Case

**7.** The 4th Respondent is opposed to the petition and relies on its Replying affidavit dated 4th March 2019.

## The 1st Interested Party's Case

**8.** The 1st interested party supports the petition and relies on its submissions dated 8th November 2018.

## The 3rd Interested Party's Case

**9.** The 3rd interested party supports the petition and relies on its written submissions dated 13th December 2018.

## Analysis and Determination

**10.** I have considered the petition, the Replying affidavit by the Respondents, Counsel rival submissions in support and in opposition of the petition as well as counsel rival oral submissions. From the aforesaid the issues arising for consideration can be summed as follows:-

a) **What are the Principles governing the interpretation of the constitution?**

b) **What are the principles for guiding court in determining whether an Act of Parliament is unconstitutional?**

**c) Whether section 5 of the Act is in violation of Article 27 of the constitution?**

**d) Whether section 22, 23, 23, 24(1) (c), 27, 28 and 37 of the Act Limit Article 32, 33 and 34 of the Constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010?**

**e) Whether sections 16, 17, 31, 32, 34, 35, 36, 38(1), 38(2), 39 and 41 of the Act are inconsistent with the constitution by failing to prescribe the mens rea element of the offence they create?**

**f) Whether section 48, 50, 51, 52 and 53 of the Act limit Article 31 of the constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010?**

**g) Whether National Assembly standing order 133 of the constitution contravenes Article 118 of the Constitution of Kenya 2010?**

**h) Whether the orders sought in the petition are in public interest?**

**A) What are the Principles governing the interpretation of the constitution?**

**11.** The petition before me entails interpretation of the constitution in determination of issues raised in this

petition. **Article 259 (1) (a) – (d) of the constitution** provides:-

> **"(1) This Constitution shall be interpreted in a manner that— (a) promotes its purposes, values and principles; (b) advances the rule of law, and the human rights and fundamental freedoms in the Bill of Rights; (c) permits the development of the law; and (d) contributes to good governance."**

**12. Article 159(2) (e) of the constitution** provides that:-

> **"(2) In exercising judicial authority, the courts and tribunals shall be guided by the following principles—**
>
> **a).....**
> **b).....**
> **c).....**
> **d).....**
>
> **e) The purpose and principles of this Constitution shall be protected and promoted."**

**13.** The court is required in interpreting the constitution, to be guided by the principle that the provisions of the constitution must be read as an integrated whole without anyone particular provision destroying the other but each sustaining the other. This proposition was enumerated in the case of **Tinyefuza vs Attorney General of Uganda**

**Constitution Petition No. 1 of 1997 (1997) UGCC 3).**

**B) What are the Principles guiding court in determining whether an Act of Parliament is unconstitutional?**

**14.** In determining whether various sections of computer misuse and Cybercrime Act are constitutional or unconstitutional the court should be guided by the principle enunciated in the case of **Ndyanabo vs Attorney General (2001) E.A. 495** in which it is provided that there is a general presumption of constitutional validity of the legislation until the contrary is proved. The burden of proof lies on the person challenging the constitutionality of the legislation to rebut this presumption.

**15.** In the case of **Susan Wambui Kaguru & others vs Attorney-General & Another (2012) eKLR,** Hon. Justice David Majaja faced with a constitutional matter rendered himself thus:-

> **"I reiterate that every statute passed by the legislature enjoys a presumption of legality and it is the duty of every Kenyan to obey the very laws that are passed by our representative in accordance with**

**their delegated sovereign authority. The question of the court is to consider whether the laws are within the four corners of the Constitution."**

**16.** The court is further required, in determining whether an Act of Parliament is unconstitutional to consider the objects and purpose of the legislation. This proposition was considered in the case of **Murage Bar Operations and Another vs Minister of State for Provisional Administration and Internal Security and others Nairobi Petition No. 3 of 2011 (2011) eKLR**

**C) Whether section 5 of the Act is in violation of Article 27 of the constitution?**

**17.** The National Computer and Cybercrimes Coordination committee is established under section 4 of the Act. According to section 5, the committee is to be composed of various public offices; in which each officer is given an option to designate a representative to the committee; which means that the committee may be made up of the officers listed in section 5; their representatives or a mixture of the latter and the former.

**18.** The petitioner's case is that as constituted, the committee violates the requirement in **Article 27(3) of the**

**Constitution;** that no more than two third of members of elective or appointive body shall be of the same gender; as section 5 of the Act, according to the petitioners, does not put in place any safeguards to ensure that the composition of the committee will be in line with Article 27 (3) of the Constitution of Kenya, 2010.

**19.** To buttress the point the petitioner avers that one of the option under Section 5 is that it is the officers listed in section 5(1) of the Act who will be members of the committee and urges that if this were to be effected during the present day, the membership of the committee would be as follows:-

| | |
|---|---|
| **a. the Principal Secretary, internal security** | **Male** |
| **b. the Principal Secretary, ICT** | **Male** |
| **c. the Attorney-General** | **Male** |
| **d. the Chief of the Kenya Defence Forces** | **Male** |
| **e. the Inspector-General of the National Police Service** | **Male** |
| **f. the Director-General, National Intelligence Service** | **Male** |
| **g. the Director-General, Communication Authority of Kenya** | **Male** |
| **h. the Director of Public Prosecutions** | **Male** |

| | |
|---|---|
| **i. the Governor of the Central Bank of Kenya** | **Male** |
| **j. the Director** | **Unknown** |

**20.** It should be borne in mind that **section 5 of the Act** establishes the National Computer and Cybercrime Co-ordination Committee in which it is clear that the respondents herein are all offices established by the constitution. The offices are constitutionally enjoined by Article 10 of the Constitution of Kenya 2010 to uphold the National Values and Principles of Governance.

**21.** Our constitution is clear that the appointment of persons to public service is governed by the provisions of Article 232 of the constitution. **Article 232(1) (i) of the constitution** is clear that the values and principles of public service include affording adequate and equal opportunities for appointment, training and advancement, at all levels of the public service of men and women. **Article 232(2) of the constitution,** provides the values and principles of public service apply to public service in all state organs in both levels of government and all state corporation, and provides that Parliament shall enact legislation to give full effect to this

Article. This provision applies equally and includes the committee set up pursuant to section 5 of the Act.

**22.** The petitioner has not demonstrated that the committee has been constituted and is in violation of provision of **Article 27 of the Constitution.** It is apparently clear that as it stands, the committee is yet to be constituted. In absence of actualization or creation of the committee, the petitioner seeks to have **section 5 of the Act** declared unconstitutional and I find the prayer is premature as there is nothing for determination. I agree with the Respondents submissions that the declaratory actions cannot be brought unless the rights in question in such action have actually been infringed. I find and hold this court does not solve hypothetical problems and abstract questions as there is no committee in place, no right has been infringed nor any is in the process of being said to be threatened. I find further the requirement of a real and actual dispute between the parties is a general limitation to the jurisdiction of the court.

**23.** I do not find any basis of the petitioner's anticipation of a potential violation of Article 27 of the constitution on un-constituted committee as a good basis that would result in

any court going beyond its jurisdiction and declare declaratory orders sought in anticipation of creation of a committee.

24. In **Republic vs. National Employment Authority & 30 others Ex-parte middle Ex-consultancy services Limited (2018) eKLR** where the Court cited with approval the finding of Kriegler J. in **Ferreira vs Levin NO & others; Vryenhoek vs Powell NO & others 1996 (1) SA 984 (CC)** at paragraph [199] to wit –

> **"The essential flaw in the applicants' cases is one of timing or, as the Americans and, occasionally the Canadians call it, "ripeness"... Suffice it to say that the doctrine of ripeness serves the useful purpose of highlighting that the business of a court is generally retrospective; it deals with situations or problems that have already ripened or crystallised, and not with prospective or hypothetical ones. Although, as Professor Sharpe points out and our Constitution acknowledges, the criteria for hearing a constitutional case are more generous than for ordinary suits, even cases for relief on constitutional grounds are not decided in the air. ...The time of this Court is too valuable to be frittered away on hypothetical fears of corporate skeletons being discovered."**

**25.** From the aforesaid I am satisfied that by constitutional fiat, judicial power operates only where there is an actual case or controversy but not in conjecture or anticipation lest the decision of this court would amount to an advisory opinion. I find to this extent the petitioner has failed to impugn the constitutionality of section 5 of the Act and I find issue (a) must fail.

**D) Whether section 22, 23, 23, 24(1) (c), 27, 28 and 37 of the Act Limit Article 32, 33 and 34 of the Constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010?**

**26. Article 33 of the Constitution of Kenya, 2010** provides thus:-

> **"(1) Every person has the right to freedom of expression, which includes—**
> **(a) Freedom to seek, receive or impart information or ideas;**
> **(b) Freedom of artistic creativity; and**
> **(c) Academic freedom and freedom of scientific research.**
>
> **(2) The right to freedom of expression does not extend to—**
> **(a) Propaganda for war;**
> **(b) Incitement to violence;**
> **(c) Hate speech; or**

**(d) Advocacy of hatred that—**

**(i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or**

**(ii) Is based on any ground of discrimination specified or contemplated in Article 27(4).**

**(3) In the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others."**

**27.** The sections quoted in the issue for determination deal with the following:-

*Section 22 – False publication,*
*Section 23 – Publication of false information,*
*Section 24 – Child pornography,*
*Section 27 – Cyber Harassment,*
*Section 28 – Cybersquatting and*
*Section 37 – Wrongful distribution of obscene or intimate images.*

The petitioners contend that section 23 of the Act is similar to section 29 of the Kenya Information and Communication Act which was declared unconstitutional in **Geoffrey Andere vs. Attorney General & 2 others (2016) eKLR.** It is urged that section 23 also reintroduces criminal defamation, formerly based on section 194 of the Penal Code; which section was

declared unconstitutional in **Jackueline Okuta & another vs. Attorney General & 2 others (2017) eKLR.**

**28.** The petitioner further argued that Article 32 of the constitution provides that every person has the right to freedom of conscience, religion, thought, belief and opinion. It is further contended Article 33 guarantees the right of every person to seek, record or report information or ideas.

**29.** The petitioner aver that the aforesaid rights echo Article 19 of both, the international convention civil and Political Rights and the Universal Declaration of Human Rights which protect the right to hold opinion without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media.

**30.** The petitioner further contend Articles 32 and 33 of the Constitution of Kenya, 2010 do not favour any type of opinion or expression and indeed offer a blanket protection for all types of ideas and expression; and rely on decisions of justice Lewis F. Pawell, in the American Supreme Court Case of **Gertz v Robert Welch Inc. 418 U.S. 323 418** come to mind:-

**"Under the First Amendment, there is no such thing as a false idea. However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries, but on the competition of other ideas."**

**31.** The petitioner contend Article 32 and 33 of the Constitution of Kenya, 2010 do not make the truth a necessary condition to the right to freedom of expression. The petitioner further argue section 22 and 23 of the Act introduce a precursor before one is entitled to their freedom of expression and as such they limit both Article 32 and 33 of the constitution.

**32.** On Adult pornography it is urged section 24 of the Act, deals with child pornography and that it is unclear whether removal of the word *"child"* before phonography in section 24(1) (c) of the Act was intentional as section 24 is titled to deal with child phonography.

**33.** In **American Booksellers Ass'n, Inc. vs. Hudnut, 598 F. Supp. 1316 (S.D. Ind. 1984)** it was held that the American First Amendment protections, which are comparable to Article 33, extend to regulation of words and pictures to the extent that they express ideas and

therefore constitute 'speech'. The court concluded that pornography is constitutionally protected speech.

**34.** In **Print Media South Africa v Minister of Home Affairs Film and Publication Board Case CCT 113/11 [2012] ZACC 22** the Constitutional Court of South Africa considered whether sexual conduct is constitutionally protected. It held that any form of expression not excluded from protection under the Constitution benefits from the preserve of the right.

**35.** The petitioner assert that forbidding the consumption and production of phonography as set out under section 24(1)(c) of the Act does therefore limit the right to freedom of expression.

**36.** Considering Article 32 of the Constitution of Kenya, 2010, it is clear that it is primary obligation of the state to exhibit neutrality toward the content of opinions and information disseminated by the citizens. To safeguard the right to freedom of expression the state does, in principle ensure that no person, groups, ideas or means of expression are excluded a priori from public discourse. The right is nonetheless not absolute.

**37. Article 24 of the Constitution of Kenya 2010,** provides for limitation of rights and fundamental freedoms. It provides thus:-

> **"(1) A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including— (a) the nature of the right or fundamental freedom;**
>
> **(b) The importance of the purpose of the limitation;**
>
> **(c) The nature and extent of the limitation;**
>
> **(d) The need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and**
>
> **(e) The relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose."**

**38.** In enjoyment of a right such as freedom of expression, the state equally has a positive duty to protect its citizens

against attacks by others. In the European Court of Human Rights in **Özgür Gündem vs. Turkey, 16 March 2000, Application No. 23144/93** observed that the genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals.

The Court went on to state:-

> **"In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States, the difficulties involved in policing modern societies and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities."**

**39.** Considering petitioner's submissions and the Respondents submissions as well as submissions by the interested

party I find that there is no doubt that freedom as a right has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of citizens while the positive content imposes an obligation on the state to take all necessary measures to protect the freedom of expression. In this regard, I find the state has a legitimate interest in ensuring the safety and integrity of information and the protection of its citizens against cybercrimes. I therefore find that state intervention in the exercise of the freedom of expression is justified in those cases in which the freedom adversely affects the right of third parties.

**40.** In considering the proportionality of limitation to the freedom of expression in section 22 of the Act, dealing with false publication, and considering the appealing characteristics internet to the web, the court considers the impact of the restrictive not only from the point of view of the private citizen, directly affected by the measure but also from the perceptive of its impact on the public at large. I find that a particular restrictive measure may seem correct if it is studied solely for the perspective of the person affected, however from a systemic digital

perspective, noting the speed with which information is shared on the internet, the court must not only consider the impact of the limitation on private citizens, but must also consider the limitation from the prospective of interoperability of the internet.

**41.** There is no doubt that proportionality encompasses an examination of the reasonableness of the legally provided measure considered in its totality, by weighing the limitation or restriction of the right, on one hand, and the aim it seeks to accomplish or the other. The petitioner has urged the right of freedom of expression has been limited but the petitioner has failed to demonstrate the extent to which the limitation is excessive in relation to the objective to protect public interest. I find that preventive protection is warranted for purpose of preventing the dissemination of information that is harmful to the public at large.

**42.** In order for the restriction to be legitimate, certain and compelling need to impose the limitation, must be clearly established. It must therefore be demonstrated that the objective in question cannot reasonably be accomplished by any other measure other than restriction of freedom of expression. In the instant petition the petitioner has

failed to demonstrate any other measure that could possibly be taken that would realize the objective of section 22 of the Act.

**43. Section 22 of the Act** provides for the offence of false publication while section 23 of the Act provides for the offence of publication of false information. A perusal of the two sections reveal that the freedom of expression is properly limited as a publisher is allowed to freely express himself but only to the extent that such information does not fall in the category set out in **section 22(2) of the Act. Section 22 of the Act** provides:-

> **"(1) A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.**
>
> **(2) Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication**

**of false, misleading or fictitious data or misinformation that —**

**(a) Is likely to —**

**(i) Propagate war; or**

**(ii) Incite persons to violence;**

**(b) constitutes hate speech;**

**(c) Advocates hatred that —**

**(i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or**

**(ii) Is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or**

**(d) Negatively affects the rights or reputations of others.**

**Section 23 of the Act provides:**

**A person who knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both."**

**44.** I find that in line with the social contract theory, it is in the best interest of government to preserve public order

and particularly so in country whose fabric is fragile like Kenya. The country has seen first-hand effect of hate speech and negative ethnicity in the past as exhibited during the 2007 – 2008 post-election violence.

**45.** There is no doubt that in cyber space, there has been a real issue on misinformation also referred to or known as publication of *"fake news"* as one Respondent points. Such false information spreads so fast on the internet; often irredeemably. Such fake information if it concerns an individual, dead or alive, it often results in anguish and pain on the individual or family in question. Some of the fake information has resulted in fear and panic amongst members of public and may create chaos, uncertainty and a threat to the national security of the country; which situation may not only escalate especially during the electioneering period but also become emotive. I find therefore that it is necessary to establish a law to regulate and control the spread of false information which could pose a threat to the national security of the country especially in a country as fragmented as ours.

**46.** The petitioner on section 23 of the Act dealing with *"publication of False information"* urges that it is similar to **section 29 of the Kenya Information and**

**communication Act** *(thereafter **"KICA")*** which it urges was declared unconstitutional in **Geoffrey Andera vs Attorney General & 2 others (supra).** The application of the two sections are substantially different, considering that **section 29 of KICA** was found by the court too broad in its application and it further observed that on ordering person using a mobile phone, or social mobile, could not have been the person contemplated in the Act as using a licensed telecommunication system and that if the intention was to protect the operator of others, then there are clear provisions in the law of Libel. Under **section 29 of KICA** it is clear the issues were two fold and secondly on the availability of other sanctions that could adequately cater for the same offence.

**47. Section 29 of KICA** can be distinguished from section 23 of the Act. Section 23 of the Act clearly and directly targets a publication of false information over a computer system as opposed to the general publication of false information. Secondly the application of section 29 of the **KICA** was specific to individuals who have licences to *"operate telecommunication system"* or to provide *telecommunication"* as may be specified in the licence". The court in that matter rightly found that the petitioner

in that petition was not a person to whom **KICA** applied. It should on the other hand, be noted section 23 of the Act, prescribes or offence relating to a computer system and is applicable to all persons. **Section 29 KICA** was found to be vague and broad for its use of the words; *grossly offensive; indecent, obscene', 'menacing character', 'annoyance', 'inconvenience', 'needless 'anxiety'.* I find that none of these words appear in **Section 23 of the Act**.

**48.** I find none of these words appear in section 23 of the Act. I note further the decision was of a concurrent jurisdiction and the words which made court to come to its conclusion are not used in **section 23 of the Act.** The words used in **section 23 of the Act** are in my view neither broad, nor are they vague. The words used should in my view be read in their proper context alongside the other words as per the rules of interpretation of statute. I find a word in a statutory provision is to be read in collocation with comparison words.

**49.** In the Supreme Court of India in **Reserve Bank of India vs. Peerless General Finance and Investment Co. Ltd. and others {1987} 1 SCC 424** observed that:-

**"Interpretation must depend on the text and the context. They are the bases of interpretation. One may well say if the text is the texture, context is what gives the colour. Neither can be ignored. Both are important. That interpretation is best which makes the textual interpretation match the contextual."**

**50.** In context, the word *"false"* as used in **Section 23 of the Act** refers to the publication of false information that is calculated or results in panic, chaos, or violence among the citizenry. *"False"* is a plain English word and it does not require a legal definition, the effect of the provision is to criminalize the publication of false information whose intention is to create panic, chaos or violence among the citizens of the Republic or which is likely to discredit reputation of a person.

**51.** The purpose and scope of the Statute and its background. The Respondent seek guidance from the finding of Mativo J. in **County Government of Kiambu & another v Senate & others [2017] eKLR** where the Court stated thus –

**"The court interprets the constitution and how legislation should apply in a particular case as no legislation unambiguously and specifically**

addresses all matters. Legislation may contain uncertainties for a variety of reasons such as:-

1. Words are imperfect symbols to communicate intent. They can be ambiguous and change in meaning over time.
2. Unforeseen situations are inevitable, and new technologies and cultures make application of existing laws difficult.
3. Uncertainties may be added to the statute in the course of enactment, such as the need to compromise or catering for certain groups."

The Court further stated –

"The other key point for the court to consider while interpreting the law is to change and adapt the law to new and unforeseen conditions. Law must change because social institutions change and in applying generalized legal doctrine, such as statutes, to the facts of specific cases uncertainties and unforeseen problems arise. As conditions change with the passage of time, some established legal solutions become outmoded. The courts should resolve these uncertainties and assist in adapting the law to new conditions.

Finally while interpreting the law, the court should bear in mind that they should make laws when necessary to make the ends of justice. Legal systems world over could not grow as has been

**the case without a great amount of judicial law making in all fields, Constitutional law, Common Law and statutory interpretation. However, to the extent that judges make laws, they should do so with wisdom and understanding. Judges should be informed on the factual data necessary to good policy making. This includes not only the facts peculiar to the controversy between the litigants before them, but also enough of an understanding of how our society works so that they can gauge the effect of the various alternative legal solutions available in deciding a case."**

**52. Section 23 of the Act** is clearly a mirror of what is already provided for under the constitution and in particular under **Article 33(3) of the constitution** which provides:-

> **"(3) In the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others."**

**53.** From the above it is clearly spelt out that libel, whether criminal or civil, is not a constitutionally protected speech. I find that the state has an obligation to protect private individuals from defamation. This cannot be allowed in allegation of exercising any freedom of expression.

**54.** In the decision of the Supreme Court of Appeal of South Africa in **Hoho vs The State (493/05) [2008] ZASCA 98 (17 September 2008).** The Appellant before the South African Supreme Court had been found guilty of criminal defamation for having 'compiled, produced and/or published' several leaflets during the period 2001 to 2002 in which he defamed various public officials. The Court was considering whether criminalization was consonant with the South African Constitution, which is very similar to the Kenyan Constitution. The Court found as follows –

> *"But the freedom of expression is not unlimited. Although it is fundamental to our democratic society it is not a paramount value. It must be construed in the context of other values such as the value of human dignity.*
> *Human dignity is stated in s 1 of the Constitution to be a foundational value of our democratic state and s 10 of the Constitution provides:*
> *'Everyone has inherent dignity and the right to have their dignity respected and protected.'*
>
> *The value of human dignity in our Constitution . . . values both the personal sense of self-worth as well as the public's estimation of the worth or value of an individual' ie an individual's reputation. In regard to the importance of protecting an individual's reputation Lord Nicholls of Birkenhead said in* ***Reynolds v***

***Times Newspapers Ltd [2001] 2 AC 127 at 201:***

*'Reputation is an integral and important part of the dignity of the individual. It also forms the basis of many decisions in a democratic society which are fundamental to its well-being: whom to employ or work for, whom to promote, whom to do business with or to vote for. Once besmirched by an unfounded allegation in a national newspaper, a reputation can be damaged forever, especially if there is no opportunity to vindicate one's reputation. When this happens, society as well as the individual is the loser. For it should not be supposed that protection of reputation is a matter of importance only to the affected individual and his family. 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. In the political field, in order to make an informed choice, the electorate needs to be able to identify the good as well as the bad.'*

*The law of defamation, both criminal and civil, is designed to protect the reputation of people. In doing so it clearly limits the right to freedom of expression. Such limitation can be consistent with the Constitution only if it can be said that 'an appropriate balance is struck between the protection of freedom of expression on the one hand, and the value of human dignity on the other'. In Khumalo that was held to be the case*

*in so far as the civil remedy for defamation is concerned."*

**55.** While comparing criminal defamation to physical assault, the Court in **Hoho v The State (supra)** found that criminal defamation was not unconstitutional stating:-

> **"It is true that there is a civil remedy available for defamation but there is also a civil remedy available for common assault, yet nobody would suggest that there is for that reason no need for the crime of common assault. There is in my view no reason why the state should oblige and prosecute in the case of a complaint in respect of an injury to a person's physical integrity but not in the case of a complaint in respect of an injury to reputation, which may have more serious and lasting effects than a physical assault. In any event, the need for the crime in addition to the civil remedy is proved by the present case. The complainants in this case did not know who was responsible for the publication of the defamatory allegations and had to enroll the assistance of the police and the prosecuting authorities to prove that it was the appellant."**

**56.** When considering cyber libel it must be distinguished from any other form of libel in regard to the speed with which defamatory statements posted in cyberspace, facilitated by one-cluck options offered by the networking site and

the quickness in dissemination of such reactions to other internet users all over the world. I find there exists a substantial distinction between libel through the use of information and communication technology and libel published using traditional means. In using technology in question, the publisher has the ability to evade identification and is able to reach a far wider audience and cause greater harm. I find that this distinction, creates and justifies a basis for criminalization of cyber libel.

**57.** The petitioner contends **Article 32 and 33** do not favour any type of opinion or expression, instead, they offer a blanket protection for all types of ideas and expression. **Article 33 (2) and 33(3)** of the Constitution of Kenya provides:-

**Article 33(2) and (3)** provides:-

> **"(2) The right to freedom of expression does not extend to—**
> **(a) Propaganda for war;**
> **(b) Incitement to violence;**
> **(c) Hate speech; or**
> **(d) Advocacy of hatred that—**
> **(i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or**

**(ii) Is based on any ground of discrimination specified or contemplated in Article 27(4).**

**(3) In the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others."**

It is clear that contrary to the petitioner's assertion Article 33(2) and 33(3) of the constitution offer a qualification on freedom of expression.

**58.** Similarly **Article 29(2) of the international convention on civil and Political Rights** offer a qualification on the freedom of expression. It provides thus:-

> **"In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in democratic society."**

**59.** The petitioner contention is that Article 32 and 33 do not make the truth a necessary condition on the right to freedom of expression and do not see the boundaries set in the Articles.

**60.** The High Court of South Africa in **Motsepe vs The State Case No. A816/2013** considered the competing interests between criminal defamation and the freedom of the media. The Court found that the prosecution of the media journalists who committed a crime of defamation is not inconsistent with the Constitution. The Court found held at paragraph 50:-

> **"Even though the defamation crime undoubtedly limits the right to freedom of expression, such limitation is reasonable and justified in an open and democratic society and consistent with the criteria laid down in Section 36 of the Constitution."**

**61.** Having considered the rival submissions I find no basis that the correct position is that the truth is not a necessary condition to the freedom of expression as falsehoods which has a potential of harming the reputation of others as well as harm and/or injure the public morality, public order and general welfare in a democratic society such as Kenya is not to say the truth is not necessary condition to freedom of expression.

**62.** I have re-considered sections 22 and 23 and argument that section 22 go beyond the limitation under Article

33(2) and that section 22(2) expands the limitation of freedom of expression to *"false, misleading or fictitious data or information"* and that the limitation of freedom of expression is neither necessary nor appropriate. It is further contended section 23 criminalizes publication of *"information that is false in print, broadcast, data or aver a computer system, that is calculated or results in panic, chaos or violates among citizens of the Republic or which is likely to discredit the reputation of a person."*

It is urged though section 23 limits freedom of expression, it fails the test of express stipulation and precision under **Article 24(2)** for statute enacted past 2010.

**63.** It argued section 23 is vague and overloaded and has a chilling effect on members of the fourth estate, whistle blower, blogger, members of the civil society, academics, political opponents, amongst others, with resultant effect that the freedom of expression and freedom of the media as guaranteed under Article 33 and 34 of the Constitution of Kenya are curtailed. It is further contended even if the sections would be complaint with Article 24(1) of the constitution, it would fail the master of Article 24(2) of the constitution since provision is vague and overloaded and is thus unclear and not specific about the right or freedom

to be limited and the nature and extent of limitation. It is therefore contended the enforcement of section 22 and 23 of the Act by the 3rd and 4th Respondents against members of public would mean the sustenance of an insidious form of ownership that impairs core values contained in Article 33(1) and 50(2) (n) of the Constitution of Kenya.

**64.** It is further urged that **Section 22 and 23 of the Act** which criminalizes the intentional false publication and publications of false information are in tandem with both Article 24(1) (d) of the constitution which provides the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the right and fundamental freedoms of others and Article 33(3) of the Constitution of Kenya which provides in exercise of the right to freedom of expression every person shall respect the right and reputation of others as well as Article 19 of the ICCPR which allows the state to introduce limitation to protect the society from false publications and protect reputation of other citizens.

**65.** It should be appreciated that while the word *"publish"* or *"publication"* is defined under **section 3(2) of the Interpretation and General Provisions Act; section**

**23 of the Act** is different from **section 194 of the Penal Code** sought to protect individual interest while on the other end, section 23 of the Act seeks to protect public interest and therefore in tandem with Article 24(1) (d) and 33(b) of the Constitution. The declaration of invalidity of section 29 of **KICA** in case of **Geoffrey Andare vs Attorney General and 2 others (2016) eKLR** and **section 194 of the Penal Code** in the case **of Jackqueline Okula & another vs Attorney General & 2 others (2017) eKLR,** in my view do not apply to section 23 and section 27 of the Act as they are different from section 29 of **KICA** and section 194 of the Penal Code, in that they clearly spell out both the actus reus and the *mens rea* and are in tandem with **Article 24 (1) (d) and 33(3) of the Constitution of Kenya, 2010.**

**66.** The petitioner aver that the removal of the word *"child"* before pornography in section 24(1) (c) of the Act was intentional and further that a literal interpretation of the Act points at the intention being that the goal was to criminalize the access of adult pornography. The petitioner further submits that pornography as defined under **section 2 of the Act** is vague and that the

outcome of such word would be that books, periodicals, motion pictures and television scenes would be a subject of criminal proceedings under **section 24(1) (c) of the Act. Section 2 of the Act** provides:-

> **"Pornography" includes the representation in books, magazines, photographs, films, and other media, telecommunication apparatus of scenes of sexual behavior that are erotic or lewd and are designed to arouse sexual interest."**

**67.** The 3rd interested party concedes that section 24 of the Act serves a legitimate aim of curbing child pornography. However the section is vaguely worded as to constitute an unjustifiable limitation to the freedom of expression. It is submitted that the *"Sexually explicit conduct"* which is an element of the offence of child pornography is not defined under the section. The net is cast wide netting both the innocent and offenders. It is therefore contended the section is void for vagueness as it does not meet the threshold of limitation provided *"by law"* under Article 24 of the constitution and that at the same time the section in its vague nature is contrary to the principle of legality in Article 50(2) (a) which forbids vague and overloaded criminal litigation.

**68.** I have considered the definition of pornography as provided under **section 2 of the Act** and I find the same as enacted to be proper. The use of the word *"includes"* in my view simply means that the definition is wide enough to recognize that the form and concern of what constitutes pornography is dynamic. I find that there cannot be one proper definition of pornography due to societal differences and subjectivity element. In the case of **Miller vs California 413 U.S.15 (1973) the Supreme Court of the United States laid out** *"basic guidelines"* for jurors in obscenity cases they include:-

> *"a) Whether the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest.*
>
> *b) Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law.*
>
> *c) Whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value."*

The court in the Miller Case *(supra)* further found that it was constitutional for different communities to articulate

different community standards in obscenity cases Chief Justice warrant Burger wrote:-

> **"To require a State to structure obscenity proceedings around evidence of a national community standard would be an exercise in futility."**

**69.** I am therefore of the view that a legal definition of what amounts to *"erotic" "lewd"* or *"designed to arouse sexual interest"* is hard to be adequately provided for, because the same is dependent on the subject and the society in context and therefore the same will still be subject to interpretation by the courts on a case by case basis. It is not incorrect to say the legislature cannot surely be required to define every single word contained in the laws they craft. I further find the fact the words *"erotic" "lewd"* or *"designed to arouse sexual interest"* have not been defined does not necessarily render the term ambiguous or vague. In Republic **vs Lucas M. Maitha Chairman Betting Control and Licensing Board & 2 others Ex-Parte Interactive Gaming and Lotteries Limited [2015] eKLR,** the interpretation of the term *"gross proceeds"* as used in the Betting Lotteries and Gaming Act Cap 131 Laws of Kenya the Betting Control

Act was in issue. The Court noted that indeed both the Betting Lotteries and Gaming Act and the Interpretation and General Provisions Act did not provide for a definition of the term. Judge G.V. Odunga at paragraph 11 however proceeded to observe that:

> **'In my view, the mere fact that the statute does not define a particular term does not necessarily render that term ambiguous"**

**70.** I find that in any event, it is a rule of statutory construction that a statute must be construed within the context in which it is used. That if the court were required to seek further assistance in trying to decipher the intention of parliament, it need not look further than at the marginal note. In section 24 of the Act the marginal note in that section clearly show the section is concerned with *"child pornography".* In support of this proposition the 1st and 3rd Respondent rely on the decision of the **Court of Appeal in commission of Lands & Another vs Coastal Aquaculture Limited [1997] eKLR** to the extent that marginal notes, often found at the side of sections in an Act, summarize the effect of the sections and have sometimes been used as an aid to construction. The Court quoted the authoritative words of

**Garth Thorton, former Deputy Legal Secretary of the East African Common Services Organization in his book "Legislative Drafting"** where he defines *"marginal notes"* as follows:

> **"The object of a marginal note is to give a concise indication of the contents of a section. A reader has only to glance quickly through the marginal notes in order to understand the framework and the scope of an Act and also to enable him to direct his attention quickly to the part of an Act which he is looking for...."**

**71.** It is clear as indicated in marginal note of section 24 of the Act, that the section criminalizes *"child pornography".*

**72.** From the foregoing, section 24 of the Act does not amount to a unreasonable and unjustifiable limitation of the freedom of expression or right to a fair trial in an open and democratic society based on human dignity and equality under Article 24 of the Constitution of Kenya, 2010. I further find under section 24 of the Act, the state is pursuing a legitimate objective and has not used means which are boarder than necessary to accomplish that objective. The constitution is not violated as the right and freedom of the members of public are limited for justifiable reason.

**73.** The petitioner contends that **section 27 of the Act** is similar to **section 29 KICA** which was declared unconstitutional in **Geoffrey Andera vs Attorney General and 2 others (2016) eKLR.** Section 27 it is urged criminalizes speech on grounds that have no proximate relationship to the grounds in Article 33(2) of the constitution, thus:-

> **"Propaganda for war, incitement to violence, hate speech and advocacy of hatred. It is further averred that the section uses subjective and vague phrases such as "apprehension or fear of violence", detrimentally effects that persons" and "indecent and grossly offensive nature."**

**74.** In the case of **Geoffrey Andera case**, Hon Lady Justice Mumbi observed that the use of *"licensed telecommunication system"* was not meant to apply to individuals and on this basis, I am satisfied the two Acts apply to different subjects and thus cannot be said to be similar. It has not been demonstrated by the petitioner that the creation of the offence of cyber harassment is not necessary as there exists another provision under Kenyan criminal Justice system that could adequately cater for the offence. I therefore find the creation of the offence of

cyber harassment is necessary and justified. It should be borne in mind section 27 of the Act is concerned with the conduct of harassment which is sought to be criminalized. The intent of law is clear that it intends to punish socially harmful conduct thus the criminal conduct of harassment. In the Supreme Court in **Giboney v. Empire Storage and Ice Co., 336 U.S. 490, 93 L. Ed. 834, 843-844 (1949)** where the Court found that certain kinds of speech have been treated as unprotected conduct, because they merely evidence a prohibited conduct. The Court stated thus:-

> **"It is true that the agreements and course of conduct here were as in most instances brought about through speaking or writing. But it has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was, in part, initiated, evidenced, or carried out by means of language, either spoken, written, or printed. Such an expansive interpretation of the constitutional guaranties of speech and press would make it practically impossible ever to enforce laws against agreements in restraint of trade as well as many other agreements and conspiracies deemed injurious to society."**

**75.** From the aforesaid I find that the freedom of expression does not extend its immunity to speech that amounts to harassment of another person.

**76.** The petitioner argues that **section 28 of the Act,** dealing with cyber-squatting, restricts the use of certain words over the internet and as such it is a limitation to the freedom of expression. It is further averred that the right to property is also impugned as the section will also interfere with the ownership of domain names.

**77.** **Section 28 of the Act** limits freedom of expression and access to information by criminalizing the offence of cyber-squatting for which the petitioner contend less restrictive alternative remedies are available including Trade mark Act, (Cap 506) and copyright Act.

**78.** The duty of the state include the duty to protect and safeguard the intellectual property and through the enactment of this section. I find the Government will be able to effectively deal with the issue of cyber-squatting. **Article 40 (5) of the Constitution of Kenya, 2010** provides:-

> **"(5) The State shall support, promote and protect the intellectual**

**property rights of the people of Kenya."**

**79.** From the above it is clear that the essence of **section 28 of the Act** is to assist the state to effectively uphold proprietary rights under the constitution; further giving the framework for the proper enforcement of intellectual property rights and more specifically in the cyber space. It is clear that Parliament in its wisdom, elected to prescribe that criminal liability can be pursued regarding violations of intellectual property and prescribed a penalty for the same.

**80.** In the instant petition, the petitioner has failed to demonstrate how any fundamental freedom is violated in punishing what are essentially universally condemned acts for cyber-squatting. I have considered section 28 of the Act and I find that the section does not encroach on Articles 32, 35, or 33 of the Constitution of Kenya, 2010; as the section punishes what is essentially theft; thus the act of intentionally and without right making use of the things or innovation that belong to others. I find that section 28 of the Act is reasonable and justified in penalizing the use of another person's intellectual property without authority or knowledge or right,

especially where the offender uses the same in bad faith; to gain profit, or unjust encroachment, mislead, destroy reputation, or deprive the owner of the rightful opportunity to utilize their intellectual property. I find the challenge to constitutionality of section 28 of the Act, on the grounds that it limits the freedom of expression to be unfounded or without basis.

**81.** The petitioner on, **section 37 of the Act** dealing with the wrongful distribution of obscene or intimate images, contends the section prescribes a certain expression and as such it limits the freedom of expression. It is further averred the section limits the freedom of expression on grounds that it strays beyond the orbit of limitations in Article 33(2) of the constitution.

**82.** It is petitioner's contention that the words *"obscene"* or *"intimate"* are not defined and that they differ from jurisdiction to another and therefore that there is lack of clarity failing the first test under **Article 24 of the constitution** to prescribe a limitation precisely.

**83.** The petitioner in support of its proposition referred to the case of **Republic vs. Oakes, [1986] 1 S.C.R. 103** on what factors to consider when carrying out such an analysis. There it was held:-

*"To establish that a limit is reasonable and demonstrably justified in a free and democratic society, two central criteria must be satisfied. First, the objective, which the measures responsible for a limit on a Charter right or freedom are designed to serve, must be "of sufficient importance to warrant overriding a constitutionally protected right or freedom": R. v. Big M Drug Mart Ltd., supra, at p. 352. The standard must be high in order to ensure that objectives which are trivial or discordant with the principles integral to a free and democratic society do not gain s. 1 protection. It is necessary, at a minimum, that an objective relate to concerns which are pressing and substantial in a free and democratic society before it can be characterized as sufficiently important.*

*Second, once a sufficiently significant objective is recognized, then the party invoking s. 1 must show that the means chosen are reasonable and demonstrably justified. This involves "a form of proportionality test": R. v. Big M Drug Mart Ltd., supra, at p. 352. Although the nature of the proportionality test will vary depending on the circumstances, in each case courts will be required to balance the interests of society with those of individuals and groups. There are, in my view, three important components of a proportionality test. First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to*

*the objective in this first sense, should impair "as little as possible" the right or freedom in question:* ***R. v. Big M Drug Mart Ltd., (supra).***
*Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance."*

**84.** The petitioner is required to demonstrate the manner in which the section limits the freedom of expression other than contending that the choice or use of the words *"obscene"* and *"intimate"* are vague. This the petitioner has failed to do. It should further be noted, the words are used descriptively in reference to a state of affair and are clear and not vague.

**85.** In the case of **Miller vs California (supra)** to the extent that obscenity case law differs from jurisdiction to jurisdiction and further on a case to case basis. It thus follows that there cannot be a *'one fits all approach'* and therefore it would not be practicable to give one accepted legal definition of what constitutes *'obscene'* and *'intimate'.* The words will therefore be construed on a case to case basis through interpretation by the courts.

**86.** The offence created by **section 37 of the Act** should be observed, that it is not new as the distribution of obscene

images has always been criminalized conduct. **Section 181 of the Penal Code** prohibits trafficking in obscene publications. The only novel aspect of this section is the use of telecommunication network or other means of transferring data to a computer. From the aforesaid the presumption of constitutionality of **section 37 of the Act** is upheld. Further I note the petitioner has failed to set out, with enough precision, the manner in which **section 37 of the Act** limits the freedom of expression. It should be noted that the petitioner in its submissions and more specifically under **paragraph 79,80,88,89, 92 - 103** has clearly submitted government has legitimate aim in controlling fake news; cyber-squatting; and harassment and cyber-bulling. It is clear the petitioner agrees on the role of the government in regulating cyber harassment and cyber-squatting, however it is not demonstrated on what basis the petitioner seem to differ against the legitimate claim in the instances like controlling false publication, or child pornography. It is further conceded the protection of privacy is a legitimate interest. Having considered the rival submissions, and the relevant law I am of the view that section 22, 23, 24(1) (c); 27, 28 and 37 of the Act are constitutional. I further find that it is

the duty of the government under the social contract to protect its citizens and facilitate the highest attainable self-fulfillment.

**E. Whether sections 16, 17, 31, 32, 34, 35, 36, 38(1), 38(2), 39 and 41 of the Act are inconsistent with the constitution by failing to prescribe the mens rea element of the offence they create?**

**87.** The petitioner contend that the offences created by sections 16,17,31,32,34,35,36,38(1), 38(2), 39 and 41 of the Act lack the element of *mens rea* and therefore un constitutional.

**88.** It is petitioner's contention that there is a basic principle that *"wrongdoing must be conscious to be criminal"* and that a defendant must be *"blameworthy in mind"* before he can be found guilty. In the case of Staples **vs United States, (1994) No. 92-1441** the court held that the requirement that wrongdoing must be conscious to be criminal and that a defendant must be blameworthy in mind before he can be found guilty is a universal requirement in all mature systems of law as it enforces the ability and duty of the normal individual to choose between good and evil.

The court also held that the only offences that do not require proof of the *mens rea* element are public welfare or regulatory offences. For all other offences an accused person has the right to know the facts that make his conduct illegal even if he does not know that those facts give rise to a crime.

**89.** It is petitioner's averment that a likely effect of leaving out the *mens rea* element of an offence is that a broad range of apparently innocent conduct as is the case with sections 16,17,27,31,32,34,35,36,38(1), 38(2), 39 and 41 of the Act. It is further argued the offence created under the Act carry with them hefty sentences and as such cannot be said to be regulating in nature. It is further submitted that unless there is a clear statement from legislature that *mens rea* is not required, the court should not apply the public welfare rationale. It is further submitted nothing show that the National Assembly sought to create offences with no *mens rea.*

**90.** The 1st and 3rd Respondents in response to the petitioners assertion aver that in **Republic Balakrishna Pillai vs. State of Kerala, Criminal Appeal No. 372 of 2001,** the Indian court addressed its mind to the question of

*mens rea* vis-à-vis criminal offences. While quoting Blackstone, the court observed that:

> ***"To consider yet another aspect, the general principle of criminal jurisprudence is that element of mens rea and intention must accompany the culpable act or conduct of the accused. In respect of this mental element generally, the Blackstone's Criminal Practice describes it as under:***
> **"In addition to proving that the accused satisfied the definition of the actus reus of the particular crime charged, the prosecution must also prove mens rea, i.e., that the accused had the necessary mental state or degree of fault at the relevant time. Lord Hailsham of St Marylebone said in Director of Public Prosecutions v. Morgan [1976] AC 182 at p.213 : 'The beginning of wisdom in all the "mens rea" cases is as was pointed out by Stephen J in Tolson (1889) 23 QBD 168 at p.185, that 'mens rea' means a number of quite different things in relation to different crimes'. Thus one must turn to the definition of particular crimes to ascertain the precise mens rea required for specific offences.**
>
> **"Criminal offences vary in that some may require intention as the mens rea, some require only recklessness or some other state of mind and some are even satisfied**

**by negligence. The variety in fact goes considerably further than this in that not only do different offences make use of different types of mental element, but also they utilise those elements in different ways."**

**91.** From the extract it is therefore demonstrated that it is widely accepted that different offences have different elements of *mens rea.* In the instant petition, the impugned provisions encapsulate the mental elements of the various offences. The offences complained of in the sections are clearly computer integrity-crimes, being crimes that assault security of network, access mechanism by compromising the confidentiality, accessibility and integrity of computer systems. Among other things, they include hacking; cracking, vandalism, spying, denial of service attacks **(DOS)** and planting of viruses, trojan, and worms.

**92.** I am of the view that in respect of computer integrity crimes, the essential ingredient in determining *mens rea* on the part of the offender is that he or she must have been aware at the time of compromising the integrity of the computer that the access is unlawful and/or unauthorized. A quick consideration in all offences

complained of under the section, the *mens rea* element is present, through the use of certain words in each section; that is as follows:-

a. **Section 16 – "intentionally and without authorisation"**
b. **Section 17 – "intentionally and without authorisation"**
c. **Section 31 – "unlawfully destroys or aborts"**
d. **Section 32 – "wilfully misdirects"**
e. **Section 34 – "inducement to deliver electronic message not specifically meant for him"**
f. **Section 35 – "intentionally hides or detains"**
g. **Section 36 – "unlawfully destroys or aborts"**
h. **Section 38 (1) – "knowingly and without authority"**
i. **Section 38 (2) – "materially represents any fact"**
j. **Section 39 – "issues false electronic transactions"**
k. **Section 41 – subject to contractual agreement.**

**93.** There is no confusion in this petition that the Parliament in its legislative wisdom it criminalized these computer integrity offences. The petitioner in the instant petition, having failed to demonstrate in which of these provision infringe any right under the constitution or offend the constitution, I am of the view that the presumption of the constitutionality of these sections have not been rebutted. It is further to be noted that the offender does not need

to know that their actions will cause certain consequences, have a knowledge of the act will cause a computer to perform the function is enough.

**94.** The legislation is a function of parliament, and issues raised in this section are the legislative prerogative of Parliament in accordance with the doctrine of separation of powers. It is therefore assumed the legislative understands and appreciates the needs of the people and the law it enacts are directed to address the issues which are made manifest by the electorate. The legislature enacts laws which they consider to be reasonable for the purpose for which they are enacted.

**95.** In the case of High Court in Tanzania in **Jebra Kambole Jebra Kambole vs. The Attorney General Miscellaneous Civil Cause No. 32 of 2015**, faced with a similar challenge on the constitutionality of certain provisions of Tanzania's Cyber **Crimes Act No. 14 Of 2015.** The court had this to say on the use of the words *"intentional"* and *"unlawful":-*

> **This shows expressively that the phrases "intentional" and "unlawful" are commonly used when drafting to create offences. At the same time no any evidence has been availed in Court showing that the lack of definition or**

**circumstances expounding the offences therein, have led the law enforcers to execute their functions in an arbitrary way and thus obstructing any right thereof, or there being categorically specified anticipated danger of misusing the provisions. Consistent with the principle that a party who challenges that a particular provision is unconstitutional has to prove beyond reasonable doubt, the Petitioner has not succeeded surmounting that hurdle. On the contrary, what has been established is the fact that the words intentionally and unlawfully are commonly used and thus are phrases which need not be defined at all times. We have no doubt the Petitioner will appreciate that it is elementary understanding that unlawful is the opposite of lawful, so any illegal act is an unlawful act. The meaning of the word "intention" is very clear and has been used in various penal sanctions and is also an element leading to commission of a crime. A crime cannot be committed without intent".**

**96.** From the aforesaid, I find that sections 16,17,31,32,34,35,36,38(1), 38(2),39 and 41 are very clear and outline the *actus reus* and *mens rea* in the respective offences, none of the section offends the principle of legality. The offences created by impugned sections are clear and unambiguous. The sections are in

my view not inconsistent with the constitution as they do prescribe the *mens rea* element of the offences they create.

**F) Whether section 48, 50, 51, 52 and 53 of the Act limit Article 31 of the constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010?**

**97.** The protection of privacy has been considered of sufficient importance to warrant constitutional protection. The privacy provided for under **Article 31 of the constitution** is not absolute. It is not one of the rights that cannot, under Article 25 be limited. It is subject therefore to the limitations set out under Article 24 of the constitution which provides that a right or fundamental freedom in the Bill of right shall not be limited except by law, and only to the except that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.

**98.** **Part IV of the Act** provides for the procedures to be followed during investigation of the offences. **Section 48 (1) (b) of the Act** provides as follows:-

"(1) Where a police officer or an authorized person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data, that:-

(b) Has been acquired by a person as a result of the commission of an offence, the police officer or the authorized person may apply to the court for issue of a warrant to enter any premises to access, search and similarly seize such data."

**99. Section 50 of the Act** provides:-

"(1) Where a police officer or an authorized person has reasonable grounds to believe that:-

a)...

b) Specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation, the police officer or the authorized person may apply to court for an order."

**100. Section 51(1) of the Act** provides that:-

"1) Where a police officer or an authorized person has reasonable grounds to believe that:-

**a)...**
**b) There is a risk or vulnerability that the traffic may be modified, lost, destroyed or rendered inaccessible. The police officer or an authorized person shall serve a notice on the person who is in possession or control of the computer system requiring the person to..."**

The petitioner contends section 51 of the Act by-passes judicial authorization and as such makes such an order tantamount to search without a warrant.

**101.** In **Magajane v Chairperson, North West Gambling Board (CCT49/05) [2006] ZACC**, it was held that warrantless inspections must be reasonable. The Court articulated a three-pronged test for reasonableness: (1) there must be a substantial government interest, (2) the absence of a warrant requirement must be necessary to further the regulatory scheme and (3) the statute must serve as a constitutionally adequate substitute for a warrant. The latter part of the test requires that the statute must alert the subject of the search that the inspection is lawful and limited in scope. Additionally, the inspection must be limited in time, place and scope. Finally, the administrative inspection may not serve as a pretext to avoid the warrant requirements for criminal

searches. However, the inspections may have the same ultimate purpose as parallel criminal statutes and inspectors can discover evidence of crimes.

**102.** The petitioner further relies in the case of **Hunter vs Southam Inc. [1984] 2 S.C.R. 145** where the court emphasized the need to have judicial authorization before a search is undertaken. The court held that for the authorization procedure to be meaningful, it is necessary for the person authorizing the search to be able to assess the conflicting interests of the state and the individual in an entirely neutral and impartial manner. He must not be someone charged with investigative or prosecutorial functions under the relevant statutory scheme. Second, reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search, constitutes the minimum standard.

**103.** In my view the test set out in the above mentioned cases is necessary to protect individual from unjustified state intrusions upon their privacy and its intention is to prevent unjustified searches before they happen, not simply of determining after the fact, whether they opt to have occurred in the first place. In the case of **Katz v. United**

**States, 389 U.S. 347 (1967)** where it was held bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations "only in the discretion of the police. Searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment.

**104.** The petitioner contention is that all the above-mentioned sections under this issue or sections in part IV of the Act that limit the right to privacy are constitutionally invalid. It is further urged the police officers are only required to show that they have reasonable grounds to believe the existence of evidence and that the use of the word *"shall"* it is urged ties the hands of the court. In the case of **Aids Law Project case** the Court echoed **Keroche Industries Limited vs. Kenya Revenue Authority & 5 Others Nairobi HCMA No. 743 of 2006 [2007] 2 KLR 240** where the principle of legality was appreciated thus:-

> **"One of the ingredients of the rule of law is certainty of law. Surely the most focused deprivations of individual interest in life, liberty or property must be accompanied by sufficient procedural**

**safeguards that ensure certainty and regularity of law. This is a vision and a value recognized by our Constitution and it is an important pillar of the rule of law."**

**105.** In **Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd (CCT1/00) [2000] ZACC 12** the court held that the right to privacy becomes more intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from that core.

The petitioner in view of the aforesaid is of the view that subscriber data, traffic data and content data ought to be treated differently urging subscriber information is the least intimate, followed by traffic data; whereas content data is magnifying glass of the most intimate details of the individual; therefore their treatment should be different in law and should be hard to obtain. It is therefore contended section 48,50,51,52 and 53 of the Act, will disproportionately limit the right to privacy, through its attempt to bypass judicial oversight by making it optional to apply for a court order while searching and seizing data stored on a computer system.

**106.** Article 31 of the constitution provides that every individual has a right not to have their person, home or property searched. However under Article 24 of the constitution this right can be limited to the extent that the limitation is reasonable and justifiable in an open democratic society. It should be borne in mind that one of the most important tools in the prevention investigation and detection of a crime and collection and gathering of evidence is a search warrant. Search warrants are not peculiar to the computer misuse and Cybercrimes Act 2018. **Section 118 of the Criminal Procedure Code (Cap 75) Laws of Kenya and section 19 of the Police Act** provides for search warrants. Section 48,50,51,52 and 53 of the Act relate to search and seizure, disclose of data, expedited prosecution, disclosure and collection of traffic data and content data.

**107.** The computer misuse and offences conducted in the cyberspace are different from the ordinary crimes and in their very nature unique. In view of that, it follows that investigative procedures in respect of these crimes must be tailor-made to meet these unique circumstances that such crimes posit. The enactment of the impugned sections is to ensure that the law enforcement officers

conduct their duties efficiently and in real time as effective investigation of cybercrime is not possible without adequate investigative powers. The limitation imposed in my view is necessary for the purposes of ensuring that an individual does not curtail the rights and freedoms of others, public peace and public morality.

**108.** In determining the constitutionality of procedures of investigating officers under the Act, the court should take judicial notice of the following aspects of computer systems:-

*i) By their nature, attributing ownership and authorship of electronically stored information (ESI) and identifying individuals in control computer systems is difficult.*

*ii) Data in computer system is stored in voluminous sets. Expediently locating relevant information amongst those voluminous sets of data is almost impossible sometimes.*

*iii) Tracing criminal activity where data anonymization and obfuscation techniques are employed, which is often the case is, more often than not an exercise in futility.*

*iv) The widespread availability of sanitization and data wiping software leads to destruction of evidence. It is therefore vital that evidence*

*stored in computer systems is retrieved within the shortest time possible.*

v) *There exists great difficulty in obtaining authorization for search and seizure in respect of data stored remotely, particularly in relation to Cloud Service Providers.*

vi) *A very low proportion of offences conducted in the cyber space are brought to the attention of law enforcement. Resultantly, whereas there is widespread manifestation of cybercrime there is concomitant widespread underreporting.*

vii) *The 'force multiplier' effect of the internet allowing offending at an unprecedented scale, given the number of internet users.*

viii) *A majority of cybercrime investigations are of a trans-national nature where an element or substantial effect of the offence is in one territory and the modus operandi of the offence is in another territory.*

ix) *Digital forensics concerned with recovering often volatile and easily contaminated information that may have evidential value, may require the use of forensic techniques include the creation of 'bit-for-bit' copies of stored and deleted information, 'write-blocking' in order to ensure that original information is not changed, and cryptographic file 'hashes,' or digital signatures, that can demonstrate changes in information.*

**109.** The aim of section 48 of the Act is to facilitate the prevention of, detection, investigation, prosecution and punishment of cyber-crime, which purpose can only be achieved through an application to the court to acquire a search warrant which enables the officer to search and seizure stored computer data. In my view the balance between achieving the purpose of the search and seizure is achieved by issuing the officer with warrant that only allows them to access data pertaining to their investigation. This would result in protecting the privacy of data of the people not relevant to the investigation. The warrant is not automatically given as the court has to consider the grounds in support and as presented by the officer when issuing the warrant. The search and seizure of computer data is contingent upon the issuance of a search warrant by court. No search can take effect under the section without court issuing the warrant. I therefore find the process is subject to judicial oversight.

**110.** The importance of a warrant issued by the court in permitting an officer to search and seize stored data was emphasized by the U.S Supreme Court in the case of **Johnson vs United State, 333 U.S. 10, 13–14 (1948)** the Court held,

**"The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers.....When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent."**

**111.** Upon clear perusal of **section 48 of the Act** it turns out that it contains built in safeguard which ensure that due process is followed; these are as follows:-

a) **The requirement that a police officer must obtain a search warrant before conducting a search;**

**b) The officer must present the court with reasonable grounds to believe that the information they seek to obtain is pertinent to their investigation;**

**c) The officer is required to present a copy of the warrant to the person against whom it is issued;**

**d) The warrant shall be in force until it is executed or cancelled by the court that issued it.**

**112. Section 50 of the Act** provides that a police officer who has reasonable grounds to believe that a person within the Kenyan territory is in possession of computer data or a data storage medium or where a service provider is in possession of specified subscriber information, the officer may apply to court for a production order.

The purpose of this section is to facilitate the prevention of, detection, investigation, prosecution and punish cyber-crime and prevent use of computer systems. The purpose is achieved through issuing a production order to persons with specified computer data or service providers with specified subscriber information in order for them to avail the information to the officer.

**113.** The section impugned contrary to the petitioner's assertion, the court is not obliged to grant a production

order. The issuance of the order is contingent upon the officer providing the court with sufficient grounds for doing so and as such it is not correct as submitted by the petitioner, that the court is denied the opportunity to exercise its discretion in making its decision. It is not automatic any application by police officer under the section should be granted.

**114.** **Section 50** provides safeguard to ensure due process is fallowed as follows:-

> **"a) A police officer or authorized person is required to obtain a Production order from the Court prior to accessing specified data stored in a computer system or specified subscriber information.**
>
> **b) The officer must present reasonable grounds to the Court to warrant the issuance of the order.**
>
> **c) The data or subscriber information to be obtained by the officer is specified i.e. he/she may only obtain information that is pertinent to the investigation."**

**115.** The 1st and 3rd Respondents relies in the case of Supreme Court of Canada in **R. v. Vice Media Canada Inc. [2018] SCC 53** where the court affirmed the legality of

the police obtaining *ex parte* production order compelling media organization and journalist to hand over instant messages exchanged with a suspected terrorist. The Court agreed that Vice had to give police the screenshots, noting that while it was important for media to be able to gather and share news with the public without government interference, in this case, public interest in investigating and prosecuting crimes outweighed it. The Court found that the judge must look at all the facts and circumstances. She/he has to balance society's interest in investigating and prosecuting crimes against the media's right to privacy in gathering and sharing news.

**116. Section 51 of the Act** allows police officers to issue a notice to a person to undertake expeditious preservation of traffic data where there is a likely of loss, modification or destruction of the data. The section proceeds to further provide that the information that is to be disclosed to the police officer is with regard to communication that would enable the identifying the service providers as the path through which the communication was transmitted. The purpose of the sections sanctioned by the section is to protect and preserve vulnerable computer data that may otherwise be lost, modified or destroyed. It therefore

follows the means through which this is achieved are rationally connected to the purpose as the police officer serve notice to persons in possession of the traffic data to undertake expedited preservation of such data.

**117.** It is petitioner's argument that **section 51 of the Act** by-passes judicial authorization by making the order tantamount to a search without a warrant. **What do section 51 of the Act do?** Section 51 allows the officer to serve notice to the person in possession of the traffic data only to undertake expeditious preservation of traffic data. The information that is disclosed to the officer is that which enables them to identify the service provider and the path through where communication was transmitted and the same do not as such by-pass authorization.

**118.** On close look at the section, it is clear that it provides safeguards to ensure due process is followed by laying down the following process:-

**a) An officer is only permitted to serve notice for the expedited preservation of specified traffic data;**

**b) A limit is given with regard to the amount of data that may be disclosed to the officer. The data is that which would be sufficient to identify the service providers**

**and the path through which communication was transmitted;**

**c) The data that is specified in the notice is to be preserved and its integrity maintained for a period not exceeding thirty (30) days;**

**d) The period of preservation may only be extended upon issuance of a Court order. The Court must be satisfied with several grounds provided for under the Section before issuing the order.**

**119.** The Court in **Kentucky v. King, 563 U. S. 452, 460 (2011)** (quoting **Mincey v. Arizona, 437 U. S. 385, 394 (1978)** stated,

> **"The needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment. Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence."**

**120.** Further, the three Judge bench of the High Court in Tanzania in **Jamii Media Company Limited –v- The Attorney General and Another, Miscellaneous Civil Cause No. 9 of 2016** faced with a similar challenge to the constitutionality of a similar Section of their Cybercrime Act which empowers police to issue disclosure

orders for purposes of investigation and/or prosecution of offences. The Court held the provision to be constitutional and that the same did not infringe the right to privacy, by finding that the safeguards in the impugned sections were sufficient. The Court opined as follows:-

> **"We have earlier stated that the Act came to address these gaps. We are asking ourselves whether the Act is unreasonable in requiring 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."**

**121. Section 52 of the Act** authorizes a police officer who has reasonable grounds to believe that traffic data associated with specified communication and relating to a person under investigation to make an application for a court order permitting them to collect the traffic data in real-time or compel a service provider with the technical capability to either collect the data or assist the police officer in its collection. **Subsection (2)** thereof further provides the grounds which the officer must satisfy in order for the court to grant the order.

**122.Section 52(3) of the Act** provides that once the Court is satisfied with the grounds that have been presented by the officer it has the authority to issue a court order permitting the collection of real-time traffic data for a period of up to six months.

**123.**The purpose of the Section is to allow a police officer to collect or record traffic data associated with specified communication and relating to a person under investigation which is required for a specific investigation in real-time. The measures undertaken by the officer are rationally connected to the purpose as the order obtained by the officer permits them to collect or record traffic data in real-time through technical means. It also permits them to compel a service provider to collector or record the data or assist the officer in the collection of the data. The measures undertaken are of the utmost necessity as there are no other means that can be employed by a police officer in collecting the traffic data in real-time.

**124.**An officer is required to provide sufficient grounds as enumerated in **Section 52(2) of the Act** to the Court before the order is granted. The balance is further achieved by limiting the period within which the officer may collect the data in real-time to six months.

**125.** The petitioner's contention as regards section 57 of the Act is that it violates right to privacy in a manner that is inconsistent with Article 24 of the Constitution of Kenya, 2010. The section has laid down safeguards to ensure due process as follows:-

a) *An officer is required to obtain a Court order allowing him/her to collect or record traffic data in real-time or compel a service provider to collect or assist the officer in the collection of the data;*

b) *The Court must be satisfied with the grounds and explanations provided for under* ***Section 52(2) of the Act*** *before issuing the order;*

c) *The Section also limits the time within which the officer may collect traffic data in real time to six (6) months;*

d) *An extension of the time given in (c) above may be given once the Court is satisfied that there are reasonable grounds to grant the same. These grounds are provided for under* ***Section 52(5) of the Act****;*

e) *In granting the order, the Court may require the service provider to keep confidential the order and execution of any power provided under* ***Section 52 of the Act****.*

In view of the safeguards provided under the section, I find the section does not limit the right to privacy as

contended by the petitioner in a manner that is inconsistent with **Article 24 of the Constitution.**

**126.** Under **Section 53(1) of the Act,** a police officer who has reasonable grounds to believe that the content of any specifically identified electronic communication is required for a specific investigation relating to an offence may make an application to court for an order permitting the officer to either collect or record content data through the application of technical means or compel a service provider with technical capability to assist him or her with the collection of the content data in real-time.

**127.** **Section 53(2) of the Act** sets out the grounds with which the Court must be satisfied before granting the order.

**128.** The purpose of the Section is to assist a police officer in obtaining the content of any specifically identified electronic communication which is required for a specific investigation. The measures undertaken by the officer are rationally connected to the purpose as the order obtained by the officer permits them to collect or record content data in real-time through technical means. It also permits them to compel a service provider to collector or record the data or assist the officer in the collection of the data.

The measures undertaken are of the utmost necessity as there are no other means that can be employed by a police officer in intercepting content data in real-time.

**129.** **Section 53(2) of the Act** requires the officer to provide sufficient grounds as enumerated in **Section 53(2)** to the Court before the order to intercept content data is granted. The period within which the officer may intercept real-time data is limited to nine months.

**130.** It is clear from the impugned section that it provides for access to specific data and thus protecting the privacy of other users, customers and third parties who are not part of the investigation. This therefore clearly prevents the infringement of the right to privacy of persons not under investigation.

**131.** The safeguards provided by the section to ensure that due process is followed include:

**a) An officer is required to obtain a Court order allowing him/her to collect or record content data in real-time or compel a service provider to collect or assist the officer in the collection of the data;**

**b) The Court must be satisfied with the grounds and explanations provided for under Section 53(2) of the Act before issuing the order;**

**c) The time within which the officer may collect content data in real time has been limited to nine (9) months;**

**d) An extension of the time given in (c) above may be given once the Court is satisfied that there are reasonable grounds to grant the same. These grounds are provided for under Section 53(5) of the Act.**

**e) In granting the order, the Court may require the service provider to keep confidential the order and execution of any power provided under Section 52 of the Act.**

**132.** Upon consideration of the impugned sections 48,50,51,52 and 53 of the Act as well as Article 37 of the Constitution of Kenya, I find that the impugned sections contain adequate safeguards to ensure the rights of the individual are well balanced as against the rights of the public in the investigation of offences under the Act. I find that the petitioner has failed to demonstrate that any right has been infringed or is threatened with infringement. Further accordingly section 3 of the Act does not give the limitation of right to privacy as one of its objects. I find the petitioner's argument that it should have been

included in the objects of the Act, cannot make a statute unconstitutional.

**G) Whether National Assembly standing order 133 of the constitution contravenes Article 118 of the Constitution of Kenya 2010?**

**133.** The petitioner contends that the National Assembly is bound by the National values and principles in Article 10 of the Constitution of Kenya, 2010 when enacting the law. That participation of the people, transparency and accountability are some of the values the National Assembly must adhere to in carrying out its legislative function.

**134. Article 118 of the Constitution of Kenya, 2010** requires the National Assembly to facilitate public participation and involvement in its business. **Article 118(1) (a) and (b) and (2) of the Constitution of Kenya 2010** provides:-

> **"(1) Parliament shall—**
> **(a) Conduct its business in an open manner, and its sittings and those of its committees shall be open to the public; and**
> **(b) Facilitate public participation and involvement in the legislative and other**

**business of Parliament and its committees.**

**(2) Parliament may not exclude the public, or any media, from any sitting unless in exceptional circumstances the relevant Speaker has determined that there are justifiable reasons for the exclusion."**

**135.** The petitioner further aver that standing order 133 provides for the committee of the whole procedure;

**i) That once a Bill is read a first time it is committed to the relevant committee which is to facilitate public participation.**

**ii) During Committee of the Whole, individual members of Parliament are nevertheless allowed to introduce new Clauses to the Bill.**

**iii) The Committee of the Whole procedure is a circumvention of the public participation procedure in Standing Order 127.**

**136.** It is petitioner's contention therefore that section 23, 31,32,33,34,35,36,37,38,39,40,41,42 and 45 of the Act were not subjected to public participation as they were introduced by individual members during committee of the whole. It is contended by the petitioner that order 133 is unconstitutional to the extent that it allows the

National Assembly to enact laws without subjecting them to public participation.

**137.** It is petitioner's assertion that the enactment of computer misuse and Cyber-Crime Act contravened standing orders 131 and 133. Standing order 131 provided that:-

> **"Where after a Bill has been read a Second Time and before commencement of Committee of the whole, amendments have been proposed to it, which in the opinion of the Speaker require harmonization, the Speaker may direct any Member proposing an amendment to be Bill to appear before the relevant Department Committee dealing with subject matter of the Bill to present his or her proposed amendments and the Committee shall submit a report to the House on the result of the exercise before the Committee of the whole House is taken."**

Standing order 133 provides that:-

> **(1) The Clerk shall call severally each part of the Bill in the sequence specified in Standing Order 132 (sequence to be observed on a Bill in committee) and if no amendment is proposed or when all proposed amendments have been disposed of, the Chairperson shall propose the question "That, ... (as amended) stand part of the Bill" and, when Members who wish to speak have spoken, the**

**Chairperson shall put that question to the Committee for decision.**

**(2) No amendment shall be moved to any part of a Bill by any Member, other than the Member in charge of the Bill, unless written given to the Clerk twenty-four hours before the commencement of the sitting at which that part of the Bill is considered in Committee.**

**(3) Despite paragraph (2), where an amendment has been moved to any part of a Bill in accordance with this paragraph, any Member may move an amendment to that amendment on delivering to the Chairperson the term of his or her amendment in writing.**

**(4) A member moving an amendment or a further amendment to any part of the Bill under paragraph (2) and (3) shall explain the meaning, purpose and effect of the proposed amendment or further amendment."**

**138.** Standing Order 133 clearly allows amendments to the Bill to be introduced during the Committee of the Whole House. The only restriction is when the proposed amendments deals with a different subject or proposes to unreasonably or unduly expand the subject of the Bill or if the amendments are inconsistent with any part of the Bill. The Petitioner has not identified with a certain degree of precision which of the proposed amendments

unreasonably expand or are inconsistent with any part of the Bill already upon. Instead, the Petitioner is reading the Standing Orders selectively. Consequently, the National Assembly complied with Standing Order 131 in introducing the amendments to the Computer Misuse and Cybercrimes Bill during the Committee of the whole house.

**139.** In the instant petition, the 2nd respondent has demonstrated that there was notice from member for Kibwezi West Constituency intending to propose amendment to computer misuse and Cyber-Crime Bill at committee stage. The speaker directed the member who had submitted amendments to the Act to appear before the Department Committee on communication, information and innovation relevant committee for harmonization of the proposed amendment with the committee report. The Honourable member Hon. Musimba, indeed appeared before the committee and his proposed amendments were harmonized with the committee report as per *(annextures marked **MS-3** true copy of the National Assembly Hansard proceedings of 26th April 2018).*

**140.** The 2nd Respondent has demonstrated that the computer misuse and Cybercrime Act was passed in accordance with the constitution and the National Assembly standing orders and therefore, the National Assembly did not infringe Article 10 and 118 of the Constitution of Kenya, 2010 as well as the standing orders as alleged by the petitioner. That though some amendments were introduced at the committee stage, the same were passed pursuant to the constitution as well as the standing order.

**141.** I find to hold that every amendment moved must undergo the process of public participation that would negate and undermine the legislation process. This procedure was enunciated in the decision in the High Court in **Institute of Social Accountability & another vs National Assembly & 4 others [2015] eKLR** the Court stated that:-

> **"We are aware that during the legislative process, amendments to the Bill may be moved during the Committee Stage and to hold that every amendment moved must undergo the process of public participation would negate and undermine the legislative process. In this case, we are satisfied that the amendment moved was in substance, within the parameters of what had been subjected to public**

**participation during the review process. We find that the public was involved in the process of enactment of the CDF Act through the Task Force and review panel earlier set up by CDF Board. The amendment was within the parameters of what was in the public domain and in the circumstances we find and hold that the amendment bill did not violate the principle of public participation".**

**142.** Further the Court of Appeal in the case of **Pevans East Africa Ltd and another vs. Chairman, Betting Control and Licensing Board and others (Civil Appeal No. 11 od 2018)** the Court held as follows:-

**"It must be appreciated that the National Assembly has heard the views of the Members of public and industry stakeholders on a Bill. It is not precluded from effecting amendments to the Bill before finally passing it. Those amendments do not necessarily have to agree with the views expressed by the people who have been heard so long as the views have been taken into account. In our view, it would bring the legislative process to a complete halt and undermine Parliament's ability to discharge its constitutional mandate if after having facilitated public participation on a Bill Parliament is required to adjourn its proceedings every time a Member**

**proposes an amendment to the Bill so that further public participation can take place on the particular proposed amendment."**

**143.** I further find that the amendments moved at the Committee of the whole House were in substance within the parameters of what had been subjected to public participation when the Computer Misuse and Cybercrimes Act, 2018 was committed to the National Assembly Committee on Communication, Information and Innovation.

**144.** The principle of allowing Parliament to regulate its internal matters has been upheld by the Supreme Court of Kenya in **Speaker of the Senate & another vs Attorney General & 4 others (supra)** where the Supreme Court stated:-

**"This Court will not question each and every procedural infraction that may occur in either of the House of Parliament. The Court cannot supervise the workings of Parliament. The institutional comity between the three arms of government must not be endangered by the unwarranted intrusions into the workings of one arm by another."**

**145.** In respect of this issue, it appears the petitioner is inviting this court to infringe on the doctrine of separation of powers as the order sought would in my view infringe the role of the National Assembly under Article 94(1) as read with Article 95(3) of the Constitution and part IV of Chapter Eight of the Constitution. I further note the petitioner has failed to demonstrate how standing order No. 133 violates the constitution. Consequently the petition has failed the competency test. In the Supreme Court of Philippine in **Andres Sarmento vs The Treasurer of Philippines G.R No. 125680 & 126313 (September, 2001)** which relied on the decision in **Lacson vs. Executive Secretary, 301 SCRA 298 (1999)** for the proposition that the Court must first make a presumption of constitutionality and it was then incumbent on the person alleging that a piece of legislation was unconstitutional to establish the unconstitutionality.

**146.** The **Supreme Court of Philippines** found that to justify the nullification of a provision of statute, there must be a clear and unequivocal breach of the Constitution, not a doubtful and argumentative one. A statute, or a part thereof, will be sustained unless it is

plainly, obviously, palpably and manifestly in conflict with some provisions of the fundamental law.

**147.** It is therefore my finding that the computer misuse and Cyber-Crime Act, 2018 was passed in accordance with the constitution and the National Assembly's standing orders and hence the National Assembly did not infringe any Article of the constitution as alleged by the petitioner.

**H) Whether the orders sought in the petition are in public interest?**

**148.** The Tenth Edition of Black's Laws Dictionary at page 1425 defines *"public interest"* as:-

> **"...the general welfare of the public that warrants recognition and protection, something in which the public as a whole has stakes, especially that justifies Governmental regulation". In litigating on matters of "general public importance", an understanding of what amounts to 'public' or 'public interest' is necessary. "Public" is thus defined: concerning all members of the community; relating to or concerning people as a whole; or all members of a community; of the state; relating to or involving government and governmental agencies; rather than private corporations or industry; belonging to**

**the community as a whole, and administered through its representatives in government, e.g. public land."**

**149.** In the instant petition the imminent danger lies in inability of the Respondents to ensure national security in view of the Cyber-crimes and computer misuse offences as set out in the affidavits in opposition to the petition; consequently the need to protect the wider public from the dangers in the cyberspace outweighs the granting of the petition. Upon examination of the impugned provisions of the Act, I find the same effectively protect the public interest and as such the public interest need to be held in the highest esteem.

**150.** Having considered the petition herein, I find the same is unmerited and I proceed to make the following orders:-

**a) The computer misuse and Cybercrimes Act 2018 is valid and does not violate, infringe or threaten fundamental rights and freedoms and is justified under Article 24 of the constitution.**

**b) Sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52, and 53 of the Computer Misuse and Cybercrimes Act are constitutional and do not violate,**

**infringe and/or threaten fundamental rights and freedoms.**

**c) The petition is accordingly dismissed.**

**d) This is a public interest matter and I accordingly direct each party to bear its own costs.**

**Dated, signed** and **delivered** at **Nairobi** this **20th** day of **February, 2020.**

.....

**J .A. MAKAU**
**JUDGE**