MedCrave
Step into the World of Research
Forensic Research & Criminology International Journal

Mini Review
Open Access
CrossMark

Cybercrime and human rights: A case for the due process of internet criminals

Abstract

The internet has grown dramatically over the last few decades. It has developed to be a platform that connects billions of users world-wide. Its functions range from work to social uses. Nonetheless, the internet has also been used for criminal activities. However, the laws dealing with the regulation have not evolved as quickly as the evolution of the internet itself. One of the notable challenges is the failure of the law to deal with cyber crimes and human rights. From this prism, this paper undertakes a forensic review of the issues that arise in the prosecution of internet criminals.

Volume 6 Issue 2 - 2018

Kondo T, Katsenga NN, Zvidzayi T
University of the Western Cape, South Africa

Correspondence: Tinashe Kondo, University of the Western Cape, Rooom 120, Law Faculty, University of the Western Cape, Robert Sobukwe, Cape Town, South Africa, Tel +27613226425, Email tkondo@uwc.ac.za

Received: April 17, 2017 | **Published:** April 26, 2018

Introduction

In recent years, the expansion of the internet has been unprecedented. The internet has been used a tool for recreation, education, work, shopping, social purposes, amongst other uses. The internet has done well in connecting people to become closer to another virtually. This has created interconnectedness and interdependence in a global economy. Many things can actually be accomplished whilst one is in the comfort of their home. Notwithstanding these positives, the internet has created another medium for crime. Cybercrime poses a danger not only for internet-based businesses, but it also poses a risk for private individuals and even governments alike. For example, a study in the United States revealed that the average cost of a data breach is about $6.5 million per incident.[1] It is against this backdrop, that this the study provides insight into cybercrimes and human rights. The study begins by unpacking the definition of a cybercrime. This definition is derived from available literature. Following this, the study magnifies on international law that relate to cybercrimes. More specifically, Council of Europe's Convention on Cybercrime (Budapest Convention). Herein, a brief discussion is led as to the content and intention of this convention. Thereafter, the study highlights on the difficulties in investigating cybercrimes. Noteworthy, evidence in cybercrime investigated is said to be fragile and easily corruptible. This is owed to the fact that there are some sophisticated cyber criminals, who set up their activities such that whenever there is an attempt to obtain evidence, the hard drives self-destruct.[2] In addition to this, chain of custody of the evidence is difficult to maintain. To give further context, this study unpacks constitutional, procedural and human rights violations in the context of cybercrime investigations. This gives the opportunity for the study to explore procedural irregularities by investigating officers with regard to constitutionally enshrined rights of an accused. In essence, the questions posed are whether:

i. There has been due process, and

ii. To what extent have human rights been violated.

Finally, the study highlights on some of the measures taken by governments to tackle the issue of cybercrime. There is a need to reconcile state practices with constitutionalism, human rights and the relevant due processes. The study attempts to make recommendations by calling for reforms.

Defining and conceptualising cyber crimes

As with most publications dealing with cybercrime, this paper also begins with furnishing a definition. It is worth noting, however, that there is no standard definition of 'cybercrime'. However, prominent definitions propose that cybercrime involves any criminal activity which takes place via computers or networks. What is interesting to note is that, many times, there is less of the cyber elements and more of the traditional elements. According to Wall, many offenses already exist in the typical criminal justice system. By way of example, one can look at offenses such as paedophilia, fraud, and pornography (Wall 2007). Accordingly, there is a debate whether categories of cybercrimes should be developed or these crimes should be understood from the lens of existing crimes. It is therefore evident that, in conceptualising cybercrimes, a challenge will remain whether these crimes actually take place in the virtual world or in the real world. These interactions between the virtual and the real worlds continue to permeate confusion in the classification of cybercrimes. Wall categorises these crimes into 3 groups:

i. Computer integrity crimes (crimes against the machines),

ii. Computer assisted crimes (crimes using the machines), and

iii. Computer content crimes (cyber-pornography, cyber-violence) (Wall, 2007).

In the context of cybercrimes, these categories should be wide enough to reign in any kind of cybercrimes. Beyond this generality, there are also many different forms cybercrimes. In an eloquent piece titled 'Transformational Dimensions of Cybercrimes', Sirohi describes these forms as cybercrime variants. He then explains the major variants as being cyberstalking,[1] hacking,[2] phishing,[3] cross-site

[1]This is the use of the internet to stalk someone on the internet.

[2]Hacking entails the exploitation of a computer system or its network.

[3]Phishing involves the use of the internet to swindle people of their money.

scripting,[4] vishing[5] and cybersquatting.[6] A principal offense in the context of cybercrime is however that of hacking which involves the targeting of the computer itself.[3] This generally involves the breach of a computer or computer system, the deliberate damage or impairment and the unauthorised interception of computer data.

The international law on cybercrimes

When analysing cybercrimes, it is interesting to note on the internet, it is difficult to establish the issue of geographical boundaries and servers. Regardless, laws have been put in place to try and regulate cybercrimes. While there is no international convention, a good piece of legislation can be found in the context of the European Union. The Council of Europe adopted the Convention on Cybercrime (CETS No.185) in 2001. This is otherwise known as the Budapest Convention. It is worth noting that the Budapest Convention is, however, also open to adoption by other parties. The main objective of the convention is to provide a response to challenges being experienced as a result of growth if the digital platform. The Budapest Convention is considered the most relevant international agreement on cybercrime and electronic evidence .[4] In its preamble, the Budapest convention speaks to international co-operation in tackling cybercrimes.

This is owed to the fact that in some instances, the offenders may be domiciled in a different country from that which they actually commit the crime in. One of the challenges that is pertinent in investigating cybercrimes is that of extradition, where cooperation may be difficult to secure. It is logical, therefore, that the Budapest Convention considers it necessary for international cooperation. At the heart of the Budapest Convention, is an appreciation of the necessity to deter the misuse of networks, systems and data by providing for the criminalisation certain acts or conducts. The Convention further realises the need to respect fundamental human rights enshrined in the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties. With regard to due processes, the Convention is specific in its requirement from members who have acceded to it. Under Article 14, there is an obligation that member states adopt legislative and other measures necessary for criminal investigations or proceedings. From a human rights perspective, the Convention also creates an obligation under Article 15 to have due regard to human rights when establishing, implementing and applying of the powers and procedures. The Convention goes further to give leeway for legislation to be enacted on search and seizure of stored computer data and inception of content data under Articles 19 and 21 respectively.

The difficulty in investigating cybercrimes

The emergence of cybercrime as one of the most serious crimes around has brought new challenges to the law enforcement sector. One of the biggest challenges facing law enforcement involves the establishment of laws against cybercrime because in some jurisdictions there are no legislations or laws covering this issue.[5] This is because the issue of cybercrime is still regarded as a new phenomenon in some jurisdictions especially in third world countries where a lot of people are failing prey to cyber criminals. According to one study that was done it was found that over 100 countries did not have penal law adequate to deal with cybercrime. Another study that examined the penal laws of fifty-two countries found that thirty-three of them had not yet updated their laws to address any type of cybercrime.[5] Globally, cybercrime was the second most reported crime in 2017. Ginni Rometty, IBM's chairman, president and CEO said that, "cybercrime is the greatest threat to every company in the world."[6] According to the Cybersecurity Business Report the world in 2015 lost up to $3 trillion as a result of cybercrime.[6] The report goes on to state that the cybersecurity community and major media have largely concurred on the prediction that cybercrime damages will cost the world up to $6 trillion by 2021 if nothing is done to curb cybercrime. Despite the shocking figures, little has been done in terms of legislations or international statutes to curb these cyber criminals.

As a result of lack of laws to charge these cyber criminals, the number of cyber-attacks continues to grow annually while at the same time the litigation rates of cybercrime, both criminal and civil, are dropping.[1] In some jurisdictions there are a lot of laws written down about cybercrimes but enforcing them is another matter. It can be frustrating for the victims of such crimes when perpetrators are not brought to justice. This is because of a number of reasons that prevents law enforcement officers from conducting their duties since cybercrimes are different from the ordinary crimes they are used to dealing with. One of the main reasons why there are few successful court cases in United States is because of the requirements that are needed for one to successfully claim for breach of data. In order to have a successful lawsuit, victims of data breaches need to prove 'injury in fact' or that the harm they suffered was concrete and particularized and actual or imminent, not conjectural or hypothetical.[1] This is often hard to prove since the damage would have occurred as a result of breach of personal information. Melissa[1] also argues that the victims of cybercrime cannot prove negligence on the part of the company holding their personally identifiable information which would have been hacked by cyber criminals. McDonough goes on to point out that this legal requirement to prove 'injury in fact' prevents many cases from even forming.

There are various challenges that are experienced by law enforcement agents in taking a cybercrime case to court. The first challenge is that of attribution; it is usually very difficult to find the real person responsible for a cyber-breach.[1] This is because cyber criminals usually disguise their originating location by using various tools and methods of concealment such as virtual private networks. The second challenge that possess the greatest obstacle in taking cyber-crimes to court is the fact cyber-crimes are digital and usually span country borders.[1] A lot of hackers operate internationally and this prevents law enforcement officers from prosecuting these individuals without extradition. For example, in the United States a lot of cybercrimes that are aimed at American citizens and firms usually originates from countries like China, Russia and Romania.[1] This in a way affects the way the law enforcement officers and the FBI Cybercrime Unit that deals with cybercrimes because they do not have jurisdiction in these countries and in some instances there are no extradition treaties between these countries. As a result, catching cyber criminals becomes a very difficult task because countries like Russia provide a safe haven for cyber criminals since they do not have an extradition with United States. The FBI had to resort to offering

[4]This involves the introduction of malicious web users into webpages that are viewed by other users.

[5]The practice entails the use of the telephone system to access public information on finances in order to derive financial.

[6]With cyber-squatting, domain names are purchased for future sale.

huge amounts of money so as to catch these cyber criminals. The FBI offered $3 million for the capture of a notorious Russian hacker who had stolen a lot of money from American banks but they could not find him because no one provided them with relevant information.[1]

Another factor that also makes convictions difficult is the issue regarding the nature of evidence that is available for cybercrimes. The problem with digital evidence is that it is different from ordinary evidence since it is fragile and can be easily be lost or corrupted. Therefore the integrity of evidence and maintaining a clear chain of custody of digital evidence is a difficult task. This is not helped by the fact of that some sophisticated cybercriminals may set up their computers to automatically destroy the evidence when accessed by anyone other than themselves. The challenges involving the issue of investigating cybercrimes if not handled carefully would lead to future disputes between governments as witnessed by the recently held press statements by Great Britain and United States. These two countries are accusing the Russian government for undertaking a coordinated campaign to target and compromise of government networks, private-sector firms and critical infrastructure providers.[7]

Constitutional, procedural and human rights violations of cybercrime investigations and convictions

An interesting perspective to ponder upon is: what are the violations that occur in the context of dealing with cybercrimes. In a bid to hunt down and track criminals, many governments are violating many internet rights. For instance, there have been attempted and actual violations of the right to privacy. To illustrate this point, one may look at the failure to secure search warrants by governments when investigating cybercrimes. In the United States, the government actually attempted to enact the Stop Online Piracy Act which tried to initiate mass surveillance. This Act was however rejected by millions of Americans on the basis that there would be online censorship in the name of fighting piracy. Another issue that has been popularised in the United States of America is that of incitement. Herein, the government baits individuals predisposed to commit a particular offense into actually committing the offense. A good example is when the state encourages a hacker to hack a particular computer in exchange for money and thereafter arrest the particular individual afterwards. This to some, presents a constitutional issue. That is, had it not been for the intervention of the state, the crime would not have been committed. In the case of Riley v. California, the court held that police officers must generally secure a warrant before conducting searches on cell phones. Their reasoning was that phones generally contain more information than that contained in physical objects on the accused. By gaining such access, police can access the accused cloud services, for example, where data is stored. In Tibet, surveillance has also targeted online searches and mobile searches. Similarly, in Bejing, businesses providing internet services were mandated to install government spyware or their licenses would be terminated. This reinforces the argument that governments are not necessarily concerned about rights in a bid to try to arrest crimes on the internet. Beyond these substantive issues, challenges on the prosecution of internet offenses also permeate to procedural matters. The rights of persons of cybercrime have not been given due regard. By way of example, those convicted of internet offenses in China have been denied due process. Further to this, many of the sentences given are not commensurate to the crimes committed. For instance, Cao Haibo, was issued with an 8 year sentence for promoting democracy online. This gives rise to the argument that there needs to be clear procedures on how internet crimes are investigated, tried and sentenced.

Conclusion

The internet as a platform remains one that presents many opportunities. This notwithstanding, the internet presents a number of governance issues. Most notably is how should governments deal with internet transgressors? As discussed, the challenge begins with the unavailability of consensus on what consists of a cybercrime to what internet rights should be afforded. This uncertainty presents an opportunity for governments to violate procedures as well as rights of those affected. It is against this background, this paper proposes that there needs to be an international convention that is signed and domesticated by all countries. A vacuum in international law actually exists in this regard. While the European Union's Budapest Convention does well in articulating a number of the cyber issues, this document does not have the weight of an international document because of its inherent regional nature. The establishment of such a convention would this, *inter alia*, assist in the understanding of cybercrimes. Moreover, a uniform approach to cybercrimes is particularly useful in the sense that there are rife jurisdictional issues on the internet. At many times, the offense is of a cross border nature, therefore the imposition of different standards by different countries would render the analysis challenging.

Another suggestion to be proffered is that there should be a commitment to respect internet human rights by all states. The fact that certain transactions take place virtually does not negate the fact that human rights should still be respected. The theory on these internet human rights should accordingly be developed. States should be on the work that has been done on the United Nations Human Rights Council non-binding resolution for the promotion, protection, and enjoyment of human rights on the internet. Included in this work, should also be the contents of the Budapest Conventions as it relates to cybercrimes and human rights. Importantly, states must also be clear on the procedures to be followed in prosecuting cybercrimes. This clarity will eliminate arbitrariness and force governments to follow due process in dealing with cybercrimes. The current fogginess in the procedure to be followed incentivises states to take advantage of the opportunity to disregard due process. Closely related to this, there must also be clarity on what sentences are appropriate for internet crimes. It should however be borne in mind that, where predicate offenses exist, these should also be taken into account during sentencing.

Acknowledgements

None.

Conflict of interest

Author declares that there is no conflict of interest.

References

1. McDonough M. The Difficulties of Litigating Cyber Crime.
2. Shinder D. What makes cybercrime laws so difficult to enforce. 2011.

3. Sirohi MN. Transformational Dimensions of Cybercrime. 2015. p. 288.
4. Global Forum on Cyber Expertise. The Budapest Convention on Cybercrime: A framework for capacity building. 2016.
5. Brenner S. Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law. 2001;8(2).
6. Morgan S. Top 5 Cyber security facts, figures and statistics for 2018. 2018.
7. Johnson D. US and UK say Russia targeted network infrastructure worldwide. 2018.

Citation: Kondo T, Katsenga NN, Zvidzayi T. Cybercrime and human rights: A case for the due process of internet criminals. *Forensic Res Criminol Int J.* 2018;6(2):119–122. DOI: 10.15406/frcij.2018.06.00194