

INVESTIGATIONS OF VIRTUAL CRIMINAL CRIME AGAINST CHILDREN IN GHANA: A COMPARATIVE APPROACH

Augustine Amoako, University of South Africa
Lekubu Benard Khotso, University of South Africa
Mabusela Oupa, University of South Africa

ABSTRACT

The widespread of virtual criminal activities has cause changes and brought about a need for new investigative skills, laws and enforcement procedures to attack these obstacles. In view of the fact that virtual technological crimes committed through the information superhighway or the internet is evolving very rapidly, efficacious enforcement of virtual crime is becoming extremely challenging. Virtual crime is both national and international issues and local legislations alone cannot be able to combat the menace. It requires stringent laws, skilled personal, well established institutions, and transnational response. The aim of this research is to give a rudiments overview of virtual crimes investigation against children in Ghana and do comparative analysis and response of the legal fraternity to these crimes. It is importance for law enforcement agencies, especially the computer crimes units or the cybercrime units to have an in-depth understanding and establish the various types of virtual crimes against persons and the differences between them as well as the legal response to them, because the legal issues and criminalization of virtual crimes is an absolutely necessary for law enforcement personnel such as the police and the army to response and build effective technique and procedural investigative methods at local, national and international levels.

Keywords: virtual Crime, Internet, Investigations, Persons, Law, Legislation, Enforcement

INTRODUCTION

One of the pivotal events in human history is the invention of the computer and it is set side by side to most significant and prominent developments witnessed by human beings in the late eighteenth and early nineteenth centuries. The dawn of virtual or internet based information systems and technology has witnessed an emergence of a revolutionised transformation in the form of advancement and development of the civilized society. The advancements made by the modern technology have facilitated the community to develop and expand their communication networks thus enabling faster and easier networking along with information exchange. In the world today, virtual or cyber technology has become an essential part of our day to day life and has virtually got imbedded into it. With the expansion of use of virtual or cyber technology in almost every sphere of human life, there is virtually no room left for us to think of a life without the blessings of virtual information technology. In conjunction with such expeditious evolution and developments, the amalgamation between computers and communication systems unveil in the birth of virtual world. Virtual world, internet, digital community, cyber-world, and cyberspace are almost used to expressing or implying the same idea. The United Nation office of crime and drugs (2020) claimed that internet tools have been integrated into the business models of traffickers at every stage of the process (Fernando, 2021). It is noted that the interconnected network is seen as part of the

process of globalisation that is evidently sweeping away former realities and certainties, creating new opportunities and difficulties associated with living in a ‘shrinking’ world. United Nation office of crime and drugs (2013) posited that developing countries constitute 60 per cent of all internet users with 45 per cent of all internet users below the age of 25 years. The recognition and enthusiasm for these changes have been tempered by fears that the Internet brings with it new threats and dangers to our societal security. At the global level, law enforcement respondents to the study perceive increasing levels of virtual crime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain.

RESEARCH APPROACH AND METHODOLOGY

This research seeks to explore the state of virtual criminal crime against persons in Ghana and legal measures being used to address it. To achieve this, the research questions to aid us in gathering baseline information on the subject matter are:

1. What are the forms of virtual crimes against children in Ghana?
2. How is Ghana addressing virtual crime against children using comparative studies of anti-virtual crimes legal framework and investigation methodologies in countries that are known to have effective anti-virtual strategies in place

Creswell & Clark (2014) states that research approach are the plan and procedure to conduct research and it involves the connection of philosophy, research designs, and specific methods. Creswell (2009) indicated that a problem statement is the heart, clear statement supporting evidence of the research project that leads to the need for an in-depth research study and analysis in the particular environment to be addressed. The statement of purpose of the research provides the major objective or intent or “road map” of a study (Creswell & Poth, 2013). Likewise, Locke, Spirduso and Silverman posit that research aims need to be clear, specific and concise. Eleyan & Eleyan (2015) indicates that the existing background knowledge and the interests, motives and preferences of the researcher are the sets of factors that co-determine the clarification of the research objective. To begin with, it must be taken into account that the outermost in this study methodology is conceded as a scientific discipline and doctrinal legal discipline in implying mounting out and defining the most appropriate ways of having or showing good judgement in the subject of investigation in the study. In this study, legal methodology is used to discern law and legal phenomena of cybercrime investigations through analysis of statutory provisions and cases by application of power of reasoning and gives emphasis on analysis of legal rules, principles and doctrines.

The researcher followed a qualitative and doctrinal legal research approach and is of opinion that qualitative and doctrinal legal research approach provides answers to the research questions in this study. Analyse and clarify that, participant observation, in-depth interviews and artefact collection are the available strategies found in the qualitative approach. This research does not focus on data through questionnaires, systematic data analysis, observations and interview. The study relies mostly on library materials, which include reports, legislations, court cases, regulations, charters, and policies, amendments to legislation, academic journals, constitution, and textbooks (Chernyshev et al., 2017)

Defining Virtual Crime

Legal implications of virtual crimes requires, first, the definition of those actions that surround internet based information technology which one way or the other may cause harm and lastly the criminalization of those actions. To clearly understand the meaning of Virtual

Crime, one should first understand the meaning of the term Crime and then the meaning of Virtual Crime. Raed (2013) indicated that crime is a social problem in society and it affects thousands of people every year and casts fear whiles restricting people's freedom of movement and prevent them from participating wholeheartedly in community activities. Crime is not per se a legal term. It derives its meaning and has a connotation in the background of a society than the State as such. Thus, it defies an attempt to lay down a straight jacket definition with clearly defined boundaries. However, usually it is put synonymous to something which is "*a wrong*", "*an offence*", "*a misdemeanour*" or "*a felony*". The institute of company secretaries of India (2016).

Crime is as old and historical as the human society itself. Many ancient books, right from the pre-historic days, and mythological stories have spoken about crimes being committed by individuals; be it committed against an individual like ordinary theft and burglary or against the nation at large like the crimes of spying, treason, etc. According to Merriam Webster Dictionary, Crime is an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law, especially - a gross violation of law. Oxford English Dictionary on the other hand also define Crime as an action or activity or omission considered to be evil, shameful, or wrong; which constitutes an offence and is punishable by law. In a layman's language, a crime can be defined as an unlawful act punishable by a State or other authority. The term "*crime*" does not, under the modern criminal law, have a simple and universally accepted definition, though statutory definitions have been provided for certain purposes. The most popular view is that Crime is a category created by law; in other words, something is a crime if it is declared as such by the relevant and applicable law. One proposed definition is that a crime or an offence (or criminal offence) is an act harmful not only to an individual or individuals but also to the community, society or the State at large ("*a public wrong*"). Deducing from the definitions of the term 'Crime' above, Virtual Crime can be defined as an act or omission prohibited by law which is carried out either with the means of or where the target is a computer, computer source or computer network. There are, at present, a large number of terms, definitions and taxonomies proposed or used to describe crime involving computers. These terms include computer related crime, computer crime, Internet crime, e-crime, digital crime, technology crime, high-tech crime, online crime, electronic crime, computer misuse, and cybercrime. Virtual crime or cybercrime is necessary to delineate the outer limits of the subjects of study and to distinguish it from other or real world crime and offensive information operation. Consequently, it is basically noted that a wide range of differences at the international level usually make impossible reaching in complete accord definition of a controversial phenomenon. For instance the definition for terrorism by the international community has not been reached meanwhile more than hundred scholarly definitions of terrorism have been put forward. In similar manner, while virtual crime or cybercrime is widely considered as a new evolution of crime compared with older real world crimes, there is no internationally unanimous definition. The principal obstacle to reaching a comprehensive definition of virtual is that, internet based-information system keep evolving and therefore allows ever more innovation crimes to be committed in cyberspace (Lwin et al., 2020).

Virtual crimes are technology based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. According to Symantec Corporation virtual crime or cybercrime is any crime that is committed using a computer or network, or hardware device. This is a very broad definition that not only includes crimes that use or target computer systems and networks, but it also includes crimes that happen within a standalone hardware device or computer. Brenner & Koops (2004) classifies cybercrime into three categories: the use of a computer as a target of criminal activity (e.g., hacking,

dissemination of viruses and worms), the use of a computer as a tool or instrument used to commit a criminal activity (e.g., online fraud, harassment), and the use of a computer as incidental to the crime (e.g., data storage for a drug dealer to monitor sales and profits). Some others concur with this view Symantec Corporation (2017), Viano, Donald and Kweku. Still others however, classify cybercrime into only two categories Koenig, Lewis, and the Australian High Tech Crime Centre (2013). Similarly, the Foreign Affairs and International Trade of Canada (2006) classifies cybercrime into two categories: crime that is committed using computers and networks (examples hacking and computer viruses) and traditional crime that is facilitated through the use of computers (example child pornography and online fraud). The crimes which cover the indirect use of computers by criminals (example communication, document and data storage) are termed computer-supported crime and not cybercrime the Foreign Affairs and International Trade of Canada 2006. Likewise, the categorization by Urbas and Choo identifies two main types of cybercrime: these are crimes where the computer is a target of an offence (examples, hacking, and terrorism) and crimes where the computer is a tool in the commission of the offence (e.g., online fraud, identity theft). Urbas and Choo elaborate the second type, the computer as a tool, based upon the level of reliance on technology: computer-enabled crimes, and computer-enhanced and computer-supported crimes (Karie & Venter, 2015).

Classification of Virtual Criminal Activities and Vulnerabilities

There are different Virtual crimes which are taking place in the present world which is dominated by the Information and Communication Technology. It could be hackers vandalizing your website, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include pornography, 'denial of services' and virus attacks preventing regular traffic from reaching your website. Virtual crimes also include criminal activities carried out with the use of computers which further perpetuates different crimes, examples includes financial crimes, sale of illegal articles, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, email bombing, physically damaging the computer system. The number of Virtual Crimes committed is increasing with each passing day, and it is very difficult to find out as to what actually a Virtual crime is and what the conventional crime is. Information and communications technologies (ICTs) have drastically increased the porosity and contributed to the growth of organized crimes and an illicit global economy (Etges & Sutcliffe, 2010). The increased porosity and anonymity of the Internet have superimposed in a complex interaction that has enabled criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage to expand their operations globally. There has been an indication that Government-backed cyberwarfare in some countries and maverick hackers testing their skills have further threatened the security of the digital world. In 2019 Ghana lost \$ 105million and 9.8 million in 2018 due to internet fraud and cybercrime (Ghana Computer Emergence Response Team 2021). As of September 2021, the Cybercrime Unit of the Criminal Investigations Department (CID) of the Ghana Police Service said cyber frauds represented 45% of all cybercrime cases, making it the topmost. Cybersecurity Ventures also predict that global cybercrime cost to grow by 15 percent per year over the next five years, reaching \$ 10.5 trillion USD annually by 2025, up from \$3 trillion USD in 2015. The expansion of the Internet has led to an explosion in the market for online violent sexual pornography crimes, making it easier to create, access, and distribute images of abuse.

For example, in February 2014, Lewis Daynes, an eighteen (18) year old unemployed software engineer murdered a fourteen (14) year old boy called Breck Brednar from Redhill,

Surrey with whom he groomed online through a gaming site. Police found Brednar in Daynes flat in Grays, Essex and had been stabbed multiple times. Lewis Daynes was sentenced to life imprisonment with a minimum of 25 years (www.theguardian.com/uk). Also in 2015, attorney David Messerschmitt was murdered in a hotel room in Washington D.C. and police records indicated that David had posted a listing on Craigslist requesting a sexual encounter but was answered by two women who planned to rob him (washingtonblade.com). The above are just a few instances of what appears to be an explosion of crime and criminality related to the growth of new forms of electronic communication.

Virtual Crimes against Children

There are certain offences which affect the personality of an individual and can be defined as: Dissemination of Obscene Material/Child Pornography: It includes Indecent exposure/ Pornography (basically child pornography), hosting of website containing these prohibited materials. These obscene matters may cause harm to the mind of the child and tend to deprive or corrupt their mind. Casey (2012) posits that In addition to the criminalization of child pornography in the Cybercrime Convention, the Council of Europe's Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201) criminalizes some other computer-related activities in the area of sexual abuse, including online grooming. Grooming consists of pedophiles establishing a trust relationship with a minor to subsequently meet for sexual abuse. Online grooming, that is, using the Internet to establish trust, is criminalized by the Lanzarote Convention in Article 23 (Casey, 2012). 'Cyberspace', the realm of computerized interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities. Parents fear for their children's online safety, as they are told of perverts and paedophiles stalking the Internet's 'chat rooms' looking for victims. Community modifications wrought by Internet technologies 'makes the future appear not liable to give way and unpredictable', influencing public and political overreaction. Such 'moral panics', powered by the media, lead to an excessive and unjustified belief that particular individuals, groups or events present an urgent threat to society (Denscombe, 2010).

Legal approaches in Ghana

In Ghana, Cybersecurity Act, 2020 (Act 1038) partly aimed at protecting children and adults from the wrongful and non-consensual exposure of their intimate images in cyberspace Child pornography, revenge pornography, and the non-consensual distribution of private and intimate images have been on the ascendancy in recent times. Ghana's Cybersecurity Act, 2020 (Act 1038) responds to these issues by criminalising such conduct with stiff sanctions. Section 136 of the Electronic Transaction Act contend that any person who intentionally does any of the following acts; publishes child pornography through a computer; produces or procures child pornography for the purpose of its publication through a computer system; or possesses child pornography in a computer system or on a computer or electronic record storage medium commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

Also the electronic Transaction Act (ETA) 772 is the most related to the investigation and prosecution of digital crime against person in Ghana. Sections of the 98 of the Electronic Transaction Act 772 create what is known as "*Cyber Inspectors*". Section of 98 of the ETA empowers the cyber inspectors or law enforcement officers to arrest suspect or virtual criminal offenders, search and seize evidence in accordance with the law. The Electronic

Transaction Act 772 make noticeable the criminalisation of cyber offenses, admissibility of electronic evidence and enhance promotion of legal confidence within the internet transaction fraternity of Ghana. During the execution of cyber search warrant if the cyber inspector or the law enforcement officer reasonably believes that an offence against person has occurred under act or may be committed, the law enforcement officer may seize any computer, electronic record, program, information, document, or a thing that the warrant specified. Additionally, section 107-140 state all the offenses that are considered cybercrime under Electronic Transaction Act 772 which includes electronic trafficking, denial of service, child pornography among others (Grabosky et al., 2001).

Legal approaches in United States (US)

The United States congress passed the Communication Decency Act of 1996 (CDA), a law aimed at combating child pornography. *In matter of Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), the U.S. Supreme Court struck down those portions of the CDA that banned “indecent” and “Patently offensive” images as being unconstitutionally vague and overboard. The rest of the CDA banning transmission of obscene speech to minors remains in effect. The United States congress again passed the Child Pornography Prevention Act of 1996 (CPPA) that regulated computer-generated images but the U.S. Supreme court rejected the ban on “virtual child pornography” In *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 249-50 (2002), striking down the CPPA as overboard and unconstitutional. After the U.S. Supreme Court invalidated the CPPA, Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act). The PROTECT Act establishes stronger laws to combat child pornography and exploitation by revising and strengthening the prohibition on computer-generated child pornographic images, prohibiting any obscene materials that depict children, and providing tougher penalties compared to exiting law. In *United States v. Williams*, 553 U.S. 285 (2008), Supreme Court upheld convictions of the defendant for one count of pandering child pornography under 18 U.S.C. § 2252A (A)(3)(B) and one count of possessing pornography. Williams received concurrent 60-month prison terms on the two counts.

Legal approaches in Australia

In Australia, Federal and State/Territory level have enacted laws that prohibit child pornography and child abuse related offences. Wei (2015) posit that, for eliminating the dissemination of child pornography or child abuse content over the internet, provisions of Commonwealth’s Criminal Code (as amended) create ISPs “reporting obligation and that of the Broadcasting Services Act 1992 (as amended) then provide penalty for ISPs” failure to promptly take down child pornography or child abuse content. A mandated notice and takedown procedure has been put in place for the eradication of child pornography or child abuse content over the internet. Federal and State/Territory laws criminalise child pornography or child abuse related offences including possession, production, and sale/distribution of child pornography or child abuse materials (Wei 2015).

Wei (2015) also reveal that States and Territories are generally responsible for the enactment of child sex-related offences, including child pornography offences, but provisions relating to such offences differ between the various states, in terms of formulation of the offences and the penalties. In addition, Wei (2015) is of the opinion that the Commonwealth has also enacted child sex-related offences, including child pornography offences, directed at conducts occurring across jurisdictions, e.g. where the internet is involved. For reasons of brevity, only legislation at the Commonwealth (Federal) level is discussed in this report.

Section 473.1 of the Commonwealth's Criminal Code highlight, “*child pornography material*” is defined to cover a range of material including that which depicts or describes a person under 18 engaged or involved in a sexual pose or sexual activity and material the dominant characteristic of which depicts for a sexual purpose the sexual organs, the anal region, or the breasts of a person under 18. Section 473.1 also defines “*child abuse material*” as material that depicts or describes a person under 18 as a victim of torture, cruelty, or physical abuse and does so in a way that reasonable persons would regard as being, in all the circumstances, offensive (Wei 2015).

However, a child is defined as a person less than 18 years of age under schedule 7 to the Broadcasting Service Act 1992. As for child pornography related offences involving the use of the internet, Sections 474.19 and 474.22 of the Commonwealth's Criminal Code Act 1995 (as amended) make it an offence to use a carriage service (e.g. the internet or mobile phone) to access, cause to be transmitted, transmit, make available, publish or otherwise distribute child pornography or child abuse material (Wei, 2015). In addition, Sections 474.20 and 474.23 make it an offence to possess, control, produce, supply, or obtain child pornography or child abuse material for use via a carriage service. The maximum 45 penalty for all Commonwealth child pornography and child abuse material offences is fifteen years imprisonment. ISPs liability for child pornography or child abuse material is then regulated by Section 474.25 according to which internet service providers or internet content hosts are obliged to refer details of child pornography or child abuse material to the Australian Federal Police within a reasonable time if they are aware that they are hosting child sexual abuse material (Yadav et al., 2013).

Legal approaches in South African

One of the advanced countries on the African continent is South Africa. The South African government has enacted Children’s Act 38 (2005) to give effect to certain rights of children as contained in the Constitution and set out the principles relating to the care and protection of children. Also South Africa have Child Justice Act 75 (2008) aim to establish a criminal justice systems for children, who are in conflict with the law and are accused of committing offences, in accordance with the values underpinning the Constitution and the international obligations of the Republic (Ferdico, 2012). Child Pornography is also enshrined in the Films and Publications Act, 1996 which defines “*child pornography*” as any image, real or simulated, however created, depicting a person who is or who is shown as being under the age of 18 years, engaged in sexual conduct or a display of genitals which amounts to sexual exploitation, or participating in, or assisting another person to engage in sexual conduct which amounts to sexual exploitation or degradation of children of any other legislation; or any image, publication, depiction, description or sequence containing a visual presentation, description or representation of pornography or an act of an explicit sexual nature of a person 18 years or older, which may be disturbing or harmful to, or age-inappropriate, for children, as contemplated in the Films and Publications Act, 1996, or in terms of any other law, to a child, with or without the consent of B, is guilty of the offence of exposing or displaying or causing the exposure or display of child pornography or pornography to a child (Zareen et al., 2013).

CONCLUSION

It can be seen from the responses and examination of the child pornography laws of several countries that child sexual abuse content has been a serious concern in Ghana and around the globe. Significantly, efforts have been put in place to eradicate online

dissemination of child sexual abuse content. Several legal instruments both national and international provide a baseline legal standard for the protection of children from sexual exploitation. Almost all the countries under study have specific legislation or provisions on child sexual abuse content and ISPs' liability in relation to online child sexual abuse content, as is the case in the Ghana, U.S., UK and Australia. To be a good virtual crime investigator, you must have sufficient knowledge of the existing cybercrime laws and criminal procedures. You must also be familiar and abreast with exiting technology, virtual crimes, and the virtual criminals or the perpetrators who commit these crimes. Virtual technology is constantly evolving, however, and so are the virtual criminals who commit these crimes. Consequently, as a virtual criminal investigator, it is imperative that you stay current in your field, especially with respect to the electronic environment in which virtual criminals operate and the types of crimes that virtual criminals are perpetrating in this environment.

REFERENCES

- Brenner & Koops. (2004). Approaches to jurisdiction. *Journal of High Technology Law*, (4), 1-46.
- Casey, E. (2012). Digital evidence and computer crime: Forensic science, computers, and the internet. *Academic press*.
- Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: advances, challenges, and research opportunities. *IEEE Security & Privacy*, 15(6), 42-51.
- Creswell, J. W. (2009). Research design: Qualitative and mixed methods approaches. *London and Thousand Oaks: Sage Publications*.
- Creswell, J.W., & Clark, V.L. P. (2011). Designing and conducting mixed methods research. *Sage publications*.
- Creswell, J.W., & Poth, C.N. (2013). Qualitative inquiry and research design: Choosing among five approaches. *Sage publications*.
- Denscombe, M. (2010). *EBOOK: The good research guide: For small-scale social research projects*. McGraw-Hill Education (UK).
- Eleyan, A., & Eleyan, D. (2015). Forensic process as a service (FPaaS) for cloud computing. In *2015 European Intelligence and Security Informatics Conference*, 157-160.
- Etges, R., & Sutcliffe, E. (2010). An overview of transnational organized cyber crime. *Journal of Digital Forensic Practice*, 3(2-4), 106-114.
- Ferdico, J. N., Fradella, H.F., & Totten, C.D. (2012). Criminal procedure for the criminal justice professional. *Thomson/Wadsworth*, 672.
- Fernando, V. (2021). Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1-7.
- Grabosky, P., Smith, R.G., & Dempsey, G. (2001). Electronic theft: Unlawful acquisition in cyberspace. *Cambridge University Press*.
- Karie, N.M., & Venter, H.S. (2015). Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, 60(4), 885-893.
- Lwin, H.H., Aung, W. P., & Lin, K.K. (2020). Comparative analysis of Android mobile forensics tools. In *2020 IEEE Conference on Computer Applications (ICCA)*, 1-6.
- Raed, S. A.F. (2013). The use of technology of global positioning system (GPS) in Criminal investigation & right to privacy under the constitution and criminal legislations in Jordan: legal analysis study. *Revue internationale de droit pénal*, (3), 433-462.
- Wei, W. (2015). Online child sexual abuse content: The development of a comprehensive, transferable international internet notice and takedown system.
- Yadav, D., Mishra, M., & Prakash, S. (2013). Mobile Forensics challenges and admissibility of electronic evidences in India. In *2013 5th International Conference and Computational Intelligence and Communication Networks*, 237-242.
- Zareen, M. S., Waqar, A., & Aslam, B. (2013). Digital forensics: Latest challenges and response. In *2013 2nd National Conference on Information Assurance (NCIA)*, 21-29.

Received: 24-July-2023, Manuscript No. JLERI-23-13896; **Editor assigned:** 25-July-2023, Pre QC No. JLERI-23-13896(PQ); **Reviewed:** 11-Aug-2023, QC No. JLERI-23-13896; **Revised:** 18-Aug-2023, Manuscript No. JLERI-23-13896(R); **Published:** 23-Aug-2023