Information and communication technology, cybercrime and the administration of criminal justice system in Nigeria.

ALHAJI, B.K., HASSAN, A.S. and MOHAMMED, J.I.

2016

Information and communication technology, cybercrime and the administration of criminal justice in Nigeria

Baba Kura Alhaji*, DR A S Hassan* and Jamilu Ibn Mohammed**

* Lecturers, Faculty of Law, University of Maiduguri, Maiduguri-Borno State

** Lecturer, Faculty of Law, Yobe State University, Damaturu, Yobe State

Abstract

Information and Communication Technology (ICT) refers to technologies that provide access to information through telecommunications. ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form such as personal computers, digital television and robots. Other products include the internet, emails wireless networks, cell phones and other means of communication. Cybercrimes on the other hand, include offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly, using modem telecommunication networks. Nigeria is confronted with the challenges of cybercrimes and the problems of weak administration of the criminal justice system. However, the coming into force of two important laws in 2015 is a pointer to the fact that the menace of cybercrime in Nigeria are about to be contained. This paper while giving an overview of the nexus between these two new laws examines how their application will bring about the speedy dispensation of justice as well as a cybercrime free society.

INTRODUCTION

With the advent of technological development, communication through various media has become not only easier and faster, but comparatively accurate and reliable. Information can now be readily sent, received or accessed through computer, telephone, internet, fax, electronic mail and host of other sources. As a concept, information communication technology (ICT) is an umbrella term that includes all technologies for the purpose of manipulation and communication of information.[1] However, despite the huge benefits attributed to ICT, it has brought about a lot of challenges, including cybercrimes, a problem which Nigeria is currently battling with; especially the problem of how to successfully prosecute cyber criminals. This has been compounded by the observed inadequacies associated with the two main criminal procedure laws (Criminal Procedure Act and Criminal Procedure Code) hitherto used by Nigerian courts in determining criminal liabilities.

The reform of the administration of criminal justice in Nigeria gained momentum particularly in 2005 when the former Attorney General of the Federation, Akin Olujimi SAN, constituted the National Working Group on the glaring need to reform the Criminal Justice System in Nigeria. This effort was further encouraged by his successors to the office of Attorney General, especially during the tenure of Chief Bayo Ojo SAN. These efforts led to the promulgation of the Administration of Criminal Justice Act, 2015. What remains to be asked now is how effective will the provisions of the Administration of Criminal Justice Act, 2015 and the Cyber Crimes (Prohibition, Prevention etc.) Act, 2015 be in combatting cybercrimes in Nigeria.

[1] Sarkar, S., 'The Role of Information and Communication Technology (ICT) in Higher Education for the 21st Century', Vol. I, No. I (2012), *The Science Probe.* P. 32

THE DEFINITION AND CONCEPT OF ICT

Information Communication Technology (ICT) is an umbrella term that includes all technologies for the manipulation of information. In other words, ICT refers to technologies that provide access to information through telecommunications. Initially, ICT was originated referred to as information technology (IT) until recently when it was suggested by experts that the 'communication' component ought to be highlighted due to its significance. It was then that the concept transformed to information and communication technology.[2] The phrase ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form. These include personal computers, digital television and robots. On a broader level, ICT includes the internet, emails, wireless networks, cell phones and other means of communication.[3]

ICT has been defined as a broad based technology (including its method, management and application) that supports the creation, storage, manipulation and communication of information.[4] ICT may also be defined as the study, design, development, implementation, support or management of computer based information system especially software application and computer hardware. It entails the use of computer and information based electronic systems to input, process, store, transmit and receive data information, including texts, graphics, sounds and video as well as the ability to control machines of all kinds electronically.[5]

The term ICT, describes the integration of two previously existing disciplines: computing and telecommunications.[6] ICT therefore refers to the convergence of audio-visual and telephone networks with computer networks, and the technology encompasses a wide range of activities, ranging from data processing to remote control and monitoring of manufacturing robots. It also covers cabling infrastructure e.g. fibre optic cables, which carry voice, data and video communications.

A major offshoot of the convergence of information and communication technology is the emergence of the internet, which is a content distribution network comprising of a global system interconnected computer networks through which data is interchanged. The technology consists of millions of private and public academics, business and government networks of both local and global scope which facilitates the dissemination and exchange of information and makes diverse other forms of non-physical interaction the new reality.[7]

THE DEFINITION AND CONCEPT OF CYBERCRIME

Cybercrime is the generic name used for describing crimes committed through the use of computer and other network technology. In other words, cybercrime or computer crime is the crime that involves the use of computer and information communication technology network. Normally, in the commission of a cybercrime, the computer may have been used, or it may be the target through which the crime was committed. Cybercrimes can be defined as criminal actions resulting from or committed through the use of information communication technology (the computer or any other electronic means). Therefore, cybercrimes may include any illegal, unethical or unauthorised behaviour involving the transmission or automatic processing of data.

[2] Ajayi, I.A. and Ekundayo, H.T., 'The Application of Information Communication Technology in Nigerian Secondary Schools', Vol. 4, (2009), *International NGO Journal,* P. 281.

[3] Sarkar, S., 'The Role of Information and Communication Technology (ICT) in Higher Education for the 21st Century', Vol. I, No. I, (2012), The Science *Probe.* P. 32.

[4] Ajayi I.A. and Ekundayo, H.T., 'The Application of Information Communication Technology in Nigerian Secondary Schools', Vol. 4, (2009), *International NGO Journal,* P. 281.

[5] Ayanda, D., Eludiora, S., Amassoma, D., and Ashiru, M., 'Towards a Model of E-Learning in Nigerian Higher Institutions: An Evolutionary Software Modelling Approach', Vol. I, No. I, 2011, *Journal of Information and Knowledge Management,* P.31.

[6] Edwards C. and Savage N., *'Information Technology and the Law,* (Lagos, Macmillan, 1990) p. I.

[7] Adejokc, O.Y., 'The ICT Revolu1ion and Commercial Sectors in Nigeria: Impacts and Legal Interventions' Vol. 5, No. 2, 2012, *British Joumal of Arts and Social Sciences.* pp. 1-14. Also available at http://www.bjournal.eo.uk/BJASS.aspx, accessed on 26th April, 2015 at 9:0 I pm.

According to Halder and Jaishankar, cybercrimes include offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modem telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS or MMS).[8] Issues surrounding cybercrimes have become high-profile, particularly those that have to do with hacking, copyright infringement, child pornography, and child grooming.

There are problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.[9] Halder and Jaishankar further looked at cybercrime from the gender perspective as crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modem telecommunication networks such as internet and mobile phones. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activities crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.[10]

CLASSIFICATION OF CYBERCRIME

Cybercrime or computer crime encompasses a broad range of activities targeting various victims for various motives. Cyber criminals have deviced several means through which they lure the innocent and unsuspecting victim to divulge certain information which is ordinarily confidential. Some of the main classes of cybercrimes which include:

• Fraud and Financial Crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining financial benefits against the victim by:

i. Altering in an authorised way. This requires little technical expertise and is common in form of theft by employees altering the data before entry or entering false data, or by entering unauthorised instructions or using unauthorised processes;

ii. Altering, destroying, suppressing, or stealing output, usually to conceal authorised transactions. This is difficult to detect;

iii. Altering or deleting stored data.

Other forms of fraud may be facilitated using computer systems, which include bank fraud, carding, identity theft, extortion, and theft of classified information.

[8] Halder, D., and Jaishank:ar, K., *'Cybercrime and the Victimisation of Women:* laws, *Rights, and Obligations'* (Hershey, PA, USA, IGI Global, 2011).

[9] Ibid.

[10] 'Cyber warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', www.law.duke.edu, accessed on 4th April, 2016 at 10:36 am.

- **Cyber terrorism**

Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources by cyber terrorists against their innocent and unsuspecting victims.[11] A cyber terrorist is someone who intimidates or coerces a government or organisation to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. As such, a simple propaganda in the internet, that there will be bomb attack during the holidays can be regarded as cyber terrorism. There are also hacking activities directed towards individuals, families, organised by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruling people's lives, robberies, black mailing, etc.

- **Cyber extortion**

Cyber extortion occurs when a website, email sever, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer protection. According to the information on the net, Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their services.

- **Cyber hacking**

Hackers make use of the weakness and loopholes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on one's computer. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what one does on his or her computer and can also import files into one's computer. A hacker could install several programs on one's computer without his knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of company can also be hacked to get the secret info1mation of the future plans of the company.[12]

- **Cyber theft**

This involves the use of electronic medium to steal private and valuable information from the computer system of the victim with the motive to gain access on how to control the money of the victim. In the process, computers and communication systems are used to illegally obtain information in electronic format. Hackers crack into the systems of banks and transfer money into their own accounts. This is a major concern as large amounts of money can be stolen and illegally transferred. Credit card fraud is also common. Most of the companies and banks don’t reveal that they have been the victims of cyber theft because of the fear of losing customers and shareholders.[13] Cyber theft is the most common and the most reported of all cybercrimes. Cyber theft is a popular cybercrime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort.

- **Viruses and worm infections**

Cyber-criminals deliberately prepare certain applications and programs that once installed and run, may eventually release viruses and worms into one's computer system thereby breaking it down or making it vulnerable for other negative computer vices. Such viruses and worms are invisibly inbuilt

[11] Parker, D., *'Fighting Computer Crime',* (USA, Charles Scribner's Son, 1983).

[12] lbikunlc, F., and Eweniyi, 0., 'Approach to Cyber Security Issues in Nigeria: Challenges and Solutions', Vol. I, No. I, 2013, *International Journal of Cognitive Research in Science, Engineering and Education.*

[13] Ibid.

in such programs which are normally installed by unsuspecting computer users. Viruses and worms are major threats to normal users and companies. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loopholes in software or operating system. A Trojan horse is dicey; it appears to do one thing but does something else. The system may accept it as one thing, but upon execution it may release a virus worm or logic bomb.

- **Spamming**

This is the process through which mass electronic mails are illegally sent to other computer users for the purpose of promoting and advertising products on websites. This is generally referred to as email spam. Through such process, both the network operators and unsuspecting computer users are dangerously exposed to the technological tricks of the spammers. Email spamming is becoming a serious issue amongst businesses due to the overhead costs it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/eliminating spam mails. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.[14]

- **Phishing scam**

This is a form of financial fraud that involves a level of social engineering which requires the phishing scammer to pose as a trustworthy representative of an established organisation, commonly using the bank of the victim. In the process, the cyber-criminals send emails and short text messages to the victims falsely claiming to be an established legitimate enterprise in order to scam the users into surrendering private information that will be used for stealing the confidential identity information of the victims.

- **Website cloning**

In recent times, the menace of website cloning is creeping into the sphere of cybercrimes in Nigeria. Website cloners do take advantage of consumers that are unfamiliar with the internet or who do not know the exact web address of the legitimate company or organisation they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetuating credit fraud.

- **Cyber laundering**

This an electronic criminal transfer of illegally generated monies with the motive of hiding its sources and most likely its intended destination. Such class of cybercrime is common among public office holders who, with the aid of corrupt bank officials, transfer huge and unreasonable amounts of monies to a different country. Such stashed monies are hardly repatriated back to the country except in some peculiar circumstances. Even where it is returned to the country of origin, it is usually characterised by serious diplomatic tussle, undue technicalities and enormous financial expenditure. Cyber laundering no doubt has great negative impact on the economy of the nation where it is perpetrated.

[14] Op. cit, 19.

CYBERCRIME IN NIGERIA

The history of cybercrime is truly deep rooted in Nigeria. It remains a serious source of concern, disrespect and economical trauma for the country. Despite the enormous benefits associated with the advent of information communication technology, there are also grave challenges in form of cybercrimes bedevilling the honest use of information technology. Nigeria as a nation has experienced various but embarrassing cases of electronic scams which have tarnished the image of the country both at home and abroad. There are instances of these cybercrimes incidents in the country. Take the case of Elekwe, a diploma holder in computer science, who remained jobless for sometimes, was hired by a high profile internet scammer in Lagos State with the motive of assisting him to commit financial cybercrime. Despite the huge amount of ill-gotten money, Elekwe was eventually arrested, prosecuted and sentenced by the Nigerian authorities.

In 2006 the Sunday Punch reported the story of 24 year-old Yekini Labaika, from Osun State and a 42 year-old American nurse from Hinshaw who was in search of a Muslim lover to many, the young man deliberately deceived the victim by claiming to be an American Muslim by the name Philips Williams, working with an oil company in Nigeria and he promised to marry her. Yekini devised fraudulent means and swindled huge amount of monies from the woman. He was consequently tried, found guilty and imprisoned for sixteen and half year jail term.[15]

The incidence of cybercrimes in Nigeria is still on the increase. Several young persons, mostly living in urban areas, have imbibed the dubious habit of the use of information communication technology to defraud unsuspecting and innocent persons both in cash and materials. According to Adebusuyi,[16] the internet has helped in modernising fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of the internet cybercrime subculture in Nigeria. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud. Disturbed by this trend, Nigeria as a nation has put in place various criminal legislation with a view to combatting cybercrime.

CAUSES OF CYBERCRIMES IN NIGERIA

Like most other developing countries, Nigeria faces serious and several cybercrime challenges, the causes being connected to many factors. Such causes are both economical and socio-political in nature. One may readily admit that the factors causing cybercrime in Nigeria cannot be exhausted. However, this paper identifies the following causes:

- **Rapid Urbanisation**

Quest for greener pasture and city life have continuously served as impetuses responsible for rural-urban drift. Most youths prefer to drift from rural settlement to cities. Many a times such rural-urban drifts have resulted in the youths being left stranded in the cities without any tangible or legal job. Consequently, these youths are tempted to resort to cybercrime with the motive of obtaining benefits fraudulently. This attitude leads to serious competition amongst the populace, especially among the elites, who find cybercrime as a lucrative venture to engage in. The elites look at cybercrime as a business that requires less capital to "invest" in. These types of people are popularly called "yahoo-boys".

[15] Sunday Punch, July 16, 2006.

[16] Adebusuyi, A., 'The Internet and Emergence of Yahoo Boys Sub-Culture in Nigeria', Vol. 2, No. 2, 2008, *International Journal of Cyber Criminology*, page 368 - 381.

• Insatiable Drive for Wealth

The quest for wealth accumulation has continued to be one of causes of cybercrime. Many people are tempted to cyber-crime saga solely to amass wealth without giving consideration to the probable consequences. Pushed by the illicit desire to live in riches has made many young persons to wrongly engage in cybercrimes. According to Anah, Funmi and Julius, there exists a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return on the investment must be growing at a geometric rate with a minimal risk. Most cyber criminals require less investments and a conducive environment. Nigeria provides such an environment and many cyber criminals take advantage of that.

• Unemployment

Lack of tangible and reasonable job sometimes pushes idle youths to engage in cybercrimes. It is a common knowledge that every year thousands of youths graduate from various educational institutions without corresponding job opportunities. Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system. According to the Nigerian National Bureau of Statistics, Nigeria is saddled with almost twenty (20) million unemployed people, with about one million new entrants into the dispirited realm of the unemployed youths each year.

• Poor implementation of cybercrimes law

Over a period of time, facts abound that there are difficulties and poor implementation of cybercrimes laws in the country. One can readily argue that prior to the enactment of the Cyber Crimes (Prohibition, Prevention etc.) Act 2015, Nigeria had no specific and effective legislation to efficiently combat cybercrimes. Perhaps that was what informed Laura when she opined that African countries (including Nigeria) have been criticised for dealing inadequately with cybercrimes as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrimes.[17] Hope is in the increase that with the promulgation of the Cyber Crimes Act, 2015, if adequately implemented, the menace of cybercrime may either be eradicated or at least be reduced to the bare level in the country. For that to be achieved, Nigeria must identify the causes responsible for cybercrime and address them objectively.

THE LAW COMBATTING CYBERCRIME IN NIGERIA

Cybercrimes cannot be easily and completely eliminated, but they can be minimised. However, collaborative efforts of individuals, corporate organisations and governments could go a long way in reducing it to the minimal level. Computer users should effectively guard and protect the data contained therein. The current primary legislation dealing with cybercrimes in Nigeria is the Cybercrimes (Prohibition, Prevention, etc.), Act, 2015. The Cybercrime Act, 2015 is a national legislation applicable throughout the Federal Republic of Nigeria.[18] The Act consists of three (3) parts; part I deals with the objectives and the applicability of the Act· part II deals with the protection of critical national information infrastructure; and part III deals with offences and penalties for cybercrimes.

The main objectives of the Act as contained in part II thereof include:

[17] Laura, A., 'Cyber Crime and National Security: The Role of the Penal and Procedural Law', available on http://www.ejournalofscience.org, visited on 5th April,2016 at 1:10 pm.

[18] Section 2, Cyber Crimes (Prohibition, Prevention etc.) Act, 2015.

Provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

institutions, speedy dispensation of justice, protection of the society from crime, and the protection of the rights and interests of the suspect, the defendant, and the victim.[30]

However, it is imperative to note that unlike the other repealed procedural laws (Criminal Procedure Act and Criminal Procedure Code), the applicability of the Administration of Criminal Justice Act, 2015 is restrictive in nature. While the former laws are meant to be applied to all courts in the southern and northern Nigeria respectively, the latter is only intended to be applicable to criminal trials for offences established by an Act of the National Assembly and other offences punishable in the Federal Capital Territory.[31] Besides, the provisions of the Act are never intended to apply to Court Martials.[32]

Therefore, for the various 36 states of the Federation to adopt and apply the laudable and innovative provisions of the Administration of Criminal Justice Act, 2015, the respective States House of Assemblies need to 'domesticate' the Act to give it legal backing and to make it applicable in their respective states. Since the principal purpose of the Administration of Criminal Justice Act, 2015 is to ensure that the system of administration of criminal justice in Nigeria promotes efficient management of criminal justice institutions, speedy dispensation of justice, protection of the society from crime and protection of the rights and interests of the suspect, the defendant, and the victim, there is every need to for the Act to be applicable to all courts of the Federation to achieve these exalted goals.

The application of the Administration of Criminal Justice Act, 2015 nationwide will enormously assist in combatting cybercrimes. The concurrent application of the Administration of Criminal Justice Act and the Cyber Crimes (Prohibition, Prevention etc) Act will no doubt promote effective prevention and control of cybercrimes in the country.

CHALLENGES OF COMBATTING CYBERCRIMES IN NIGERIA

One of the serious effects of information communication technology is the myriad of challenges it poses in form of cybercrimes. Today, there are critical challenges being faced with computers being used for criminal behaviours in several ways. Firstly, a computer can be the target of cybercrime. This normally happens when a computer's confidentiality, integrity, or availability is attacked. That is services or information is being stolen, or victim computers are being damaged. Secondly, a computer can be used as a tool for committing criminal behaviour. There are plethora of crimes committed via computer includes pornography fraud, intellectual property violations, sale of illicit drugs and goods online, among others. Thirdly, a computer can be incidental to an offence. For instance, those cyber criminals who benefit from computers as a tool store their reprehensive data on the system and of course illicit drug traffickers and other criminals may as well store business contact information on their computers.

Therefore, the challenges confronting effective and efficient combatting of cybercrimes in Nigeria fit into five categories:

i. Technical challenges: the law enforcement agencies find it difficult to effectively trace arrest, prosecute and punish cyber criminals. This is made so because of the fact that cybercrimes are normally committed via computers and the location of the suspects are not only distant and obscure but also discreet.

[30] Section I (I), Administration of Criminal Justice Act, 2015.
[31] Section 2(1), Administration of Criminal Justice Act, 2015.
[32] Section 2(2), Administration of Criminal Justice Act, 2015.

ii. Legal challenges: prior to the advent of the Cyber Crimes (Prohibition, Prevention etc.) Act, 2015, there was no direct, specific and effective legislation that primarily dealt with cybercrimes in Nigeria. But with the coming of this Act, its effective implementation may assist in overcoming the deficient legal regime to combat cybercrimes.

iii. Operational challenges: there is lack of well-trained, well-equipped and well-motivated cybercrime investigators and prosecutors. Most a times the prosecution of cybercrimes are subjected to the traditional methods of prosecution which may result in discharging the accused person on technical grounds despite glaring evidence put before the court.

iv. Jurisdictional challenge: cybercrime is often associated with extraterritorial aspect that can give rise to complex jurisdictional tussle. For example the acts constituting the offence (s) may be committed in different nations thereby making it difficult to determine which country really has the jurisdiction to try the offender.

v. Evidential challenge: the question still remains whether evidence obtained through the internet and computer hard disk or software of an accused person or any centre can be admissible in court in order to help in prosecuting cybercrimes.

Although the Administration of Criminal Justice Act, 2015 allows a suspect to make confessional statement manually or by electronic means,[33] it is not yet clear if all other aspects of electronic evidence can be readily admitted in court as evidence. The Evidence Act[34] as of today is not specific and direct about the admissibility of electronic-generated evidence.

However, this paper observes that with the combined application of the Administration of Criminal Justice Act, 2015 and the Cyber Crimes (Prohibition, Prevention etc.) Act, 2015, the challenges posed by cybercrimes will be appropriately addressed.

CONCLUSION

Despite the enormous benefits associated with the use of information communication technology, there are attendant consequences resulting from its misuse. One of the serious challenges posed by the use of information communication technology is the menace of cybercrime. Cybercrimes have serious negative socio-economic effects both on the image of Nigeria and on the economy. The increasing wave of cybercrimes committed by Nigerians has no doubt portrayed the country negatively both at home and abroad. It is in view of the above that the concurrent advent of the Administration of Criminal Justice Act, 2015, and the Cyber Crime (Prohibition, Prevention etc.), Act, 2015 should be seen as a major positive departure from the traditional and ineffective system of combatting crimes in general and cybercrimes in particular. To holistically apply the provisions of these two legislations in order to combat cybercrimes the technical, legal, operational, jurisdictional and evidential challenges identified need to be adequately addressed by the authorities concerned.

[33] Section 15(4) and (5), Administration of Criminal Justice Act, 2015.

[34] Evidence Act, 2011.