GLOBAL ACADEMIC EXCELLENCE

Volume: 4 Issues: 15 [June, 2019] pp.154-165]
International Journal of Law, Government and Communication
eISSN: 0128-1763
Journal website: www.ijlgc.com

IDENTITY CRIME IN THE DIGITAL AGE: MALAYSIAN AND MAURITANIAN LEGAL FRAMEWORKS

Sidi Mohamed Sidi Ahmed
PhD Candidate, AIKOL, IIUM
(Email: kaldbkar@yahoo.com)

***Accepted date**: 05-05-2019*
***Published date**: 11-07-2019*

To cite this document: Ahmed, S. M. S. (2019). Identity Crime in The Digital Age: Malaysian and Mauritanian Legal Framework. *International Journal of Law, Government, and Communication*, 4(15), 154-165.
DOI: 10.35631/ijlgc.4150016

Abstract: *Legally speaking, a crime is an action or omission punishable by law and it takes many forms, e.g., crimes against people, property and so forth. Identity crime is one of those crimes that could affect financial institutions, individuals or even the whole society. Identity crime impacts include, inter alia, emotional and psychological, financial and security ones. In its basic meaning, identity crime is a term used to refer to all forms of unlawful activities (stealing, fraudulently using, modifying, etc.,) done under the identity of persons (names, passports, bank accounts, etc.). The term 'identity' includes all information relating to persons (natural or legal) such as name, address, email, phone number, bank account, uniform and such like. These types of crimes are not new but there is no doubt that the availability of information and data in the virtual world flourishes identity related-crimes and makes them easier to be committed. Like other countries in the world, Malaysia and Mauritania have general and specific provisions for combatting identity related-crimes and bringing offenders to justice. This paper discussed the concept of identity crime, then analysed and examined laws related to the matter in the legal systems of the two countries and assessed the efficiency and capability of those laws to combat this serious crime. Moreover, it made a comparison between the two systems and suggested some steps to be taken to improve the existing laws governing identity crime in the countries. This research is a doctrinal research depending on both primary and secondary related sources. It is argued and believed that a study such this will positively contribute to the field of legal studies as it is examining an aggravated crime (identity crime) from a comparative perspective.*

Keywords: *Identity Crime, Digital Age, Laws, Malaysia, Mauritania*

Introduction

The words of 'crimes' and criminals are well-known to both laymen and experts for their bad and harm effects on the society and its members. Identity crime is one of those crimes that could have a negative impact on financial institutions, individuals or even the whole society. In its basic meaning, identity crime is a generic or an umbrella term used to refer to all forms of unlawful activities which targeted identities (names, passports, bank accounts, emails, etc.,) of persons (natural or legal) such as identity theft, fraud and so forth. Identity related crimes are not new but there is no doubt that the availability of information and the dependence on it in the digital age flourish these types of crimes, open the appetites of the criminals and make such crimes easier to be committed than before. When criminals get personal information of someone, they can use such information in many ways such as draining bank accounts, opening new utility accounts, getting medical treatment on the victim's health insurance (Federal Trade Commission, 2019) and such like. The most dangerous and probably surprising things with identity crime could be the wide range of its victims whom could be governments, corporations and individuals regardless of their ages, gender, education, literature, income and such like (Lawson, 2011). Identity crime is not a petty crime, but it is a serious crime that could cause financial, psychological, and other impacts to its victims (The International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR), 2011). For example, the victims of this crime in the United States (US) in 2017 was 16.7 million and its cost was $17 billion (IA Pascual, 2019). Moreover, identity fraud which is part of identity crime costs the United Kingdom around £ 1.2 billion yearly (Wall, 2013). The above indicates that identity crime in the information age is a challenging problem that deserves to be legally dealt with. Thus, around the globe, laws and regulations have been enacted or revised to combat those growing crimes. Malaysia and Mauritania have general and specific provisions that can be employed to curb identity crime and bring offenders to courts. This paper attempts to discuss the concept of identity crime and then analyse and examine laws related to it in the legal systems of the two countries to assess the efficiency and capability of those laws to combat this serious new-old crime in the digital environment.

Methodology

This research is a doctrinal research depending on both primary and secondary related sources. It employs both analytical and comparative approaches to analyse and then compare some legal provisions applicable to identity crime in the two countries. It will draw a comparison between the two systems and recommend for improvement when that is relevant. This research is based on data collected from primary sources such as some statutes of the two countries. It also uses data and information of secondary sources such as books, journals, Internet databases and such like.

It is argued and believed that a study such this will positively contribute to the field of legal studies as it is discussing an aggravated crime (identity crime) from a comparative perspective.

Definition of Identity Crime

Comprehensive understanding any terminology requires knowing the meaning of its words separately and jointly. Accordingly, defining the phrase of 'identity crime', necessitates knowing the meaning of both 'identity' and 'crime.' Linguistically speaking, the word identity denotes the process of providing information about a person or an object. For example, while identity as a noun represents or explains "who you are or what your name is" and also "the qualities that make someone or something what they are and different from other people", the meaning of 'identify' as a verb is "to recognize someone and be able to say who they are" and "to recognize something and understand exactly what it is" (MACMILLAN English Dictionarry, 2002). In the academic sense, Jaishankar, asserted that identity crime is a mutual concept that can be grouped into three categories, namely a personal, social and legal identity (Jaishankar, 2008). For example, the personal identity is related "to the self as experienced by the individual" and social identity is the self in the eyes of other members of the society. The third category is the legal identity which is defined as "the way in which an accumulation of information distinguishes one individual from all others" (Jaishankar, 2008). The word crime, on the other hand, denotes "something… against the law", something… morally wrong" or "illegal behaviour in general" (Oxford Wordpower, 1999, p. 178). The legal meaning of crime is not far from the linguistic one as it is defined as "an act (or sometimes a failure to act) that is deemed by statute or by the common law to be a public wrong and is therefore punishable by the state in criminal proceedings (Oxford Dictionary of Law, 2003, p. 128). When identity and crime are combined', they are called 'identity crime', a term that "refers to all forms of wrongdoing conducted under the guise of another person's identity, as well as to preparatory acts involving the collection, manipulation and trading of identity information" (Lawson, 2011, p. 111). Moreover, one of the most comprehensive definition of identity crime could be the one that sees it as "a cycle with five distinct phases: (1) unauthorized or illegal acquisition of identifying data or items (e.g., cards or documents); (2) transfer of the initially acquired identifying data or documents; (3) manipulation of the data or items (e.g., through alteration, compilation, or forgery/counterfeiting); (4) transfer of the manipulated data or items; and (5) use of the data or items for fraud or concealment of criminal identity" (The Cross-Border Crime Forum, 2019, p. 2). The above quoted definitions include common key elements such as the object of identity crime (data or information), the act (acquiring data, using or manipulating it, etc.), mental elements (obtaining and using information, etc., indicate the mental element) and missing authorization by victims. These four mentioned elements "are required for the development of a criminal law provision in defining the structure. (Gercke, 2011, p. 31).

As can be deduced from the above, the term "identity crime" is used to refer to all unlawful activities against identities (passports, bank accounts, etc.,). Identity crime is not the only used term, but there are various terms and expressions that have been used in different places to describe misusing identities such as 'identity crime' (in Australia), 'identity theft' (in the UAS) and 'identity fraud; as in the UK (Sidi Mohamed Ould Mohamed, 2015).

This paper adopts the term identity crime and uses it as a generic term to cover various crimes against identities in different separated stages. As an illustration, identity crime here used to include all unlawful activities involving information related to persons (including legal and natural ones). Such lawful activities could be forging, altering, stealing, destroying, using and such like. The discussion will mainly focus on the legal frameworks of the studied countries (Mauritania and Malaysia). Looking identity crime in separated stages allows to judge criminal activities in distinct stages. For example, some criminals could be engaged in collecting information while others may go further and manipulate or use such information to commit further crimes. Thus, discussing identity crime in all those stages and knowing the applicable provisions, if any, could help curb those serious crimes and mitigate their bad impacts. The next paragraph will be dedicated to the nature of identity crime and its subject matter.

The Nature of Identity Crime

In the previous section it is mentioned that identity crime revolved around using identities of others for gaining unlawful benefits or committing crimes under their names. As identities and personal information become essential elements of the information age, they become a target of criminals who wish to take advantages and privilege that such identities grant to their holders. Identities or information which are targeted in identity crime depend on the nature of the crime that offenders want to commit. For example, if the perpetrator wants to steal money from a victim's account or fake identity documents, he would look for financial and personal information related to that matter. In general, information that is protected by different national laws and usually targeted by identity-criminals includes the flowing three categories: (1)

names, addresses, date of birth, marital status, death certificate, ID cards, passports, or immigration documents, drivers' licenses, social security numbers, health insurance number, fingerprint, voice print, retina image, iris image, or DNA profile; (2) credit or debit card numbers, financial institution account numbers and written signature and such like; (3) e-mail login, e-mail or web browsing passwords, mac-address or IP-address, electronic or digital signature, and usernames (Gercke, 2011). This targeted information can be divided into three categories. One is information related to the person himself (name, ID card, etc.,), information pertaining to his financial interests (bank accounts, credit card numbers, etc.,) and finally information that can be used to get or infringe his personal and financial information (e-mails, IP-address, etc).

There are various tactics that have been used by criminals to get and collect identity information. These tactics range from very simple ways to highly sophisticated ones in which the criminals use high technology to collect information. In general, identity-related information can be obtain through digital and non-digital methods. In the digital method, criminals employ various technologic tactics including, inter alia, phishing: "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (Jaishankar, 2008 , p. 11), skimming: "copying information from the magnetic strip on credit cards while they are used for purchasing goods or withdrawing money from the ATMs" (Shun-Yung Kevin Wang , 2011, p. 8), hacking: "unapproved utilization of computer and system assets" or in other words it is "the act of changing computer equipment and programming to achieve an objective outside of the maker's unique reason" (Sunil Kumar , 2018, p. 2253) and Malicious Software: "any software that are being used for disturbing normal system functions, collect important information, or can access to private computer systems" (Milan Jain , 2014).

The non-digital method includes, for instance, redirection of mail which enables offenders to access documents sent through it; theft such as theft of wallets, passports, etc., dumpster diving, shoulder surfing; listening for oral disclosures of personal identity or watching, using public available information in books or newspapers and such like, and insider attacks such as bribing employees to provide identity information about victims (Gercke, 2011).

In fact, the availability of data in the digital world and the vulnerability of such data to be leaked ease the job of identity-criminals and enable them to accumulate databases about potential victims. For example, in one of the biggest data breaches in the history, three billion of Yahoo users' "accounts were hacked in a 2013 data theft" (Jonathan Stemple , 2017). and the leaked data included names, email addresses, date of birth, telephone numbers etc (Yahoo, 2016). Regarding data breach in the studied countries and in Malaysia particularly, there was a report about the leakage of "roughly 46.2 million mobile phone numbers from Malaysian telcos and mobile virtual network operators (MVNO)" and other important databases stored by some organizations in 2017 (Lowyat.net, 2017). The same resource reported that those data is being offered for sell and thus such data becomes subject to various unlawful misuse by malicious people.

Information (identities) related to natural or legal persons can be used to commit various crimes such as identity theft, identity fraud and so forth. For example, the International Centre for Criminal Law Reform and Criminal Justice Policy (hereinafter, ICCLR) found that identity criminals can use identifying information in the following illegal activities: (1) selling identity information to other criminals for use in identity-related crime, (2) accessing and using the victims’ credit or debit cards and taking over their bank accounts, (3) opening new financial accounts, loans or mortgages in the victim’s name, (4) obtaining a passport or other identity documents in someone else’s name, obtaining government benefits and services using the victim’s name, (5) concealing their identity while travelling illegally, smuggling drugs, engaging in money-laundering, terrorism etc., and (6) misleading law enforcement or court officials by directing them to the wrong persons (The International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR), 2011).

The above usage of identities includes using them for financial and non-financial purposes. However, some reports showed that 74% of the stolen information used to commit financial identity theft crime (Identity Theft Resource Center (ITRC), 2013). Thus, types of identity crime vary depend on the usage of stolen identities by the criminals. For example, identity crime includes, among other things, identity theft and identity fraud. Identity theft and identity fraud can be used interchangeable by some or separately in which identity theft means the act of obtaining personal identity information and identity fraud refers to the act of utilizing such information by the criminals. (Shun-Yung Kevin Wang , 2011)

The discussion indicates that identity crime in the digital age could be considered one of the serious crimes that could threaten both society and its members. The coming section will look at identity crime from legal perspective.

Law and Identity Crime

Identity takes its importance from being a method or instrument that distinguishes persons or objects from each other and thus “humans make sense of the world and people understand and act toward each other depending on identities” (Sarah J. McCarthey , 2002). It (identity) has many aspects such as social, commercial, technological, and legal ones and most aspects of identities are subject to identity-related crimes. For example, the tale of Imrou‟ al-Qais (a famous Arabic poet) can be taken as an example of social identity crime in the past (Mostapha Abd al-Shafi, 2004). According to the tale, the poet swore not to marry any woman unless she answers some questions correctly. He got many wrong answers but in one dark night he met a very intelligent young lady with her father and she answered his questions perfectly. Without delay, he proposed to marry her and the proposal was accepted. At the agreed time, the poet and his helper took one hundred camels and some furnishings and went to the lady ‘s family. Unfortunately, the helper decided to commit identity crime throughout by throwing his master inside a water well and impersonating him. In the end of the drama, the helper arrived at the lady‘s house, introducing himself as the famous poet who has come for his wife (Mostapha Abd al-Shafi, 2004).

In the present era, legal identity is essential because it enables a person to enquire his rights and access to public and private services. Without a valid legal identity, one cannot easily travel or access financial or other services, etc. According to Emily Finch, legal identity serves dual purposes; it enables individuals to authenticate themselves and provides their historical continuity as individuals-here and now’ by connecting them with events in their past, e.g. credit, employment history (Finch, 2007). Due to the innumerable advantages they are granting to the holders, identities especially the legal ones are being targeted by criminals who want to benefit from the privilege they offer to the holders. As response to this, law in different parts of the globe grants some protection to identities either by special provisions or by general ones. For example, the Canadian Criminal Code (R.S.C., 1985, c. C-46-, s.402.2) criminalizes misusing of identities by stating that “everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence."

In Malaysia and Mauritania, there is no piece of law under the name of 'identity crime law', but instead some provisions of the existing laws in the countries can be employed to curb identity-related crimes as the paper aims to point out in the coming paragraphs. Identity crime, as mentioned in the definition section, includes separated crimes such as unauthorised or illegal acquisition of identifying data, manipulation of the data and use of the data for fraud or concealment of criminal identity. All these acts could be combated either by traditional provisions such as those found in Penal Codes or by especial provisions enacted for the information age such as computer crimes or data protection laws which both come to protect data including personal data in the information age. Before talking about identity crime in light of Malaysian and Mauritanian existing statutes, some similarities and dissimilarities between the two countries will be drawn in order to facilitate assessment of laws relating to identity crime in the countries' legal systems.

Technological Aspects

Regarding the development of information and communication sectors which play an important role in identity-related crimes today, when compare to Malaysia, it could be fair to say that Mauritania is suffering from the lack of advancement in technological-related sectors. The gab can clearly be seen in the percentage of the Internet users in the two countries. For example, the Internet World Stats showed that the percentage of Internet users in Mauritania and Malaysia in 2019 are 17.4 % and 77.3 % respectively (Internet Word Stats, 2019). The table below explains this is more details.

Country	Population	Internet User	Percentage
Malaysia	32,454,455	25,084,255	77.3 %
Mauritania	4,661,149	810,000	17.4 %

Table 1: Internet Users in Mauritania and Malaysia in 2019

In terms of data breach reports, statistics and press news show that there are great incidents of data leakage in Malaysia (Lowyat.net, 2017) and (Malaysia Computer Emergency Response Team (MyCERT), 2018). Moreover, it is said that one of every 10 Malaysians is affected by identity theft (RAO, 2018). In Mauritania, however, there is no available reports about data breach, but the Mauritanian press began to report stories and incidents which indicate that identity-related crimes and computer crimes in general could be a major problem that will face the country in the future. As an example, the police arrested a foreign man and a Mauritanian man and his wife in one incident of forgery. In detail of this incident, the forger claimed to be a relative of the Mauritanian couple and that his father died. After investigation, the police discovered the fact and arrested all of them (Mohamed, 2014).

Legal Systems

As opposed to the Mauritanian legal system which mostly depends on rules derived from the Islamic Shariah especially the *Maliki's* School of Thought, "the role which Islamic law now plays in the [Malaysian] system is extremely limited" (Ahmad, 2007). Another distinction between the two systems could be that while Mauritania inherited French Civil Law legal system, Malaysia inherited the Common law legal system. Keeping the above distinction in mind, the following is analyzing some aspects of identity crime such as illegal acquisition of identifying data, manipulation of the data and use of forged identities to commit crimes in both legal systems.

Collecting Identifying Data

As explained before, identity criminals have many ways and tools to obtain personal data of their victims. Some of this method are explicitly illegal such as stealing the information while others are not. In the Malaysian legal framework, there are some provisions protecting personal and financial information and prohibiting an authorised disclosure of such information and they can arguably be used to curb identity crime. One of these laws is the Computer Crimes Act (CCA) 1997 which aims "to provide for offences relating to the misuse of computers." For example, sections 3 and 4 of the CCA criminalise unauthorised access to computer materials and unauthorised access with intent to commit or facilitate further offence respectively. Moreover, section 4 of the CCA makes it is clear that commission of further offence include "an offence involving fraud or dishonesty, or which causes injury as defined in the Penal Code." These provisions seem to cover some digital methods used by criminals to collect identifying information about their victims such as hacking (Sunil Kumar , 2018) and Malicious Software (Milan Jain , 2014) because they are involving accessing computers or computer systems in unauthorised manners and as some mentioned the term unauthorised access is conventionally known as hacking. (Azmil, 1997). other important laws that can be used to combat financial-identity crime in Malaysia could be the Financial Services Act (FSA) 2013 and the Islamic Financial Services Act (IFSA) 2013. For example, these Acts prohibited disclosing information related to accounts or affairs of all customers. The prohibition includes the officers and directors of the financial institutions and others (FSA 2013, s 145; IFSA 2013, s 133.). Since financial identities such as information relating to customer accounts are the most wanted information (Identity Theft Resource Center (ITRC), 2013), it can be said that these Acts could help minimising identity crime in its first stage. Another protective mechanism could be the obligation imposed by Personal Data Protection Act (PDPA) 2010 on data users especially the disclosure and security principles. The disclosure principle (S. 8) of the Act prohibited disclosing personal data without the consent of the data subject for any purpose other than the collected purpose and its related purposes. The principle serves the fight against identity crime in that it can prevent or at least minimise the inside jobs (disclosing personal information by the staff). Moreover, the security principle obliges data users to take practical steps to secure the data (PDPA, s. 9).

In Mauritanian side, there are also provisions of laws that can be used to combat identity crime in its early stages. Accordingly, some traditional laws such as the Penal Code (July 9- 1983) and the penal provisions found in other especial laws will generally govern matters relating to identity crime and cybercrimes in the country. In this regard, the criminal provisions mentioned in the Mauritanian Code of Civil Status (hereinafter the Code) (Law No. 2011-003, issued on January 12, 2011) can act as a preventive tool against identity crime in its first stage: collecting identities. This Code aims to establish and organise the procedure and conditions related to issuing and recording events of civil status (birth, marriage, divorce, death, etc.) and secured documents related to that status (s. 1 of the Code). For example, the Code explains and organises the way of issuing identity-related documents, criminalises providing false statement or perjury therein and prohibits submitting personal information to anyone other than the owner or his legal agent or representative (s. 26 and 63 of the Code). All these can arguably help minimise identity crime as it helps keep identity-related information in the right hand.

Additionally, the Code imposes heavy penalties on offenders. As an example, punishments for making false statement or witness for issuing false documents are imprisonment for a term range from six to ten years and a fine of 2.500.000 to 4.000.000 of the Mauritanian currency, Ouguiya (MRO) in addition to civil right deprivation. Moreover, issuing documents to those who are not entitled to them is a crime that is punishable by imprisonment (of five to eight years) and fine (range from 2.2000.000 to 3.5000.000 of MRO) as well as deprivation of civil rights. Moreover, the Code also imposes double of the above punishments in cases where the crime is committed by an officer or the beneficiary is a foreigner. Additionally, the Mauritanian Law No. 007-2016 Concerning cybercrimes also comes with some provisions that can be used to combat identity crime in the virtual word. For example, section 4 of this cybercrimes law prohibits interception of information and punishes such act by imprisonment and fine. Moreover, section 6 of it also prohibits unauthorised access to computer systems and punishes such act. These various laws could help protect identities from leakage to criminals' hands and then bring identity-criminals to justice in case of any breach those regulatory rules.

Bearing in mind that identity crime starts with the acquisition of victims' information, the above provisions are arguably useful tools offered by the legal systems of Malaysia and Mauritania and those laws can be used to curb identity crime in the digital age as they help protecting information from being leaked and fallen into criminal hands.

Forging and Using Identifying Data

Identity-criminals collect information about their targeted victims to use it in fraudulent ways with or without changing it. For example, passports and others travelling documents are usually targeted by criminals because they enable offenders to facilitate travel after committing crime or help them initiate new ones as well as to avoid prosecution in multiple jurisdictions (The Cross-Border Crime Forum, 2019). Fortunately, these types of crimes can fall under laws such as the Malaysian Passport Act 1966 which criminalises using forged passport or internal travel document, impersonation or representing oneself falsely; and knowingly producing false document for gaining passports (s 12 & 12B). All these and other provisions such as those in the Malaysian Births and Deaths Registration Act 1957 criminalising forging birth-certificates (s. 36) could fight identity crime. The birth certificate is one of the identification documents that are usually targeted by identity criminals. Another important piece of law that can help combat identity crime in Malaysia is the Penal Code which prohibits fraud, impersonation, and forgery. For example, section 463 of the Penal Code defines forgery to include any person who makes false document or part of a document with the intention to commit fraud.

In its side, Mauritania has some provisions that can apply to some identity-criminal activities in the real world such as forging and using forged identities. Such provisions could be useful as criminals have used forged identities to deceive and gain undeserved benefits and privilege. For instance, several Articles of the Mauritanian Penal Code are devoted to forgery crimes. As an illustration, Articles 149 and 150 make it illegal to forge or use forged identity documents including travel documents such as passports and visas etc. and impose harsh punishments on those who are involved in the process of forgery. In the Code, the term 'forgery' includes, inter alia, false statements, impersonating false names or attributes, and giving false information (section 150). The wider scope of this definition and the variety of the documents included in it could be useful in fighting against identity-related crimes because these crimes can virtually include all types of identities. For the forgers, punishments range from imprisonment (6 months to 3 years) and fine (MRO 5,000-150,000). Regarding gaining and using false identities, the punishments also include imprisonment (3 months to 2 years) and fine (MRO, 5,000 to 50,000).

In one rare reported identity crime case in Mauritania, a Mauritanian woman sentenced to imprisonment for one year and a fine of two million of MRO after committing the crime of forgery (Mohamed, 2014). In this case, the Court of Misdemeanors found that the convicted woman sold identity of her dead daughter to a foreign woman to enable her to register as the woman's daughter and get the Mauritanian nationality. This case could have an important impact on the issue of identity crime in the country because it may help bring the attention of stakeholders (law enforcement, judge, legislative bodies, etc.,) in the country to new types of crimes (buying and selling identities). Furthermore, general provisions relating to violation of the Shariah are another tool that can be used to curb identity crime in the absence of special Mauritanian laws in the matter. For example, Article 306 of the Penal Code mentioned that anyone who violates the sanctity of the Shariah (the sanctity of Allah) or helps others to do so shall be punished. The term 'violation of the sanctity of the Shariah' includes doing any prohibited thing or refraining from doing any obligation. If Article 306 reads in light of Article 449 of the Penal Code which referred to the Shariah in all matters that omitted in the Code, it can be also argued that the Article (Art. 306) can be applied to all issues violating the Shariah including identity-related crimes that violate established Shariah rules.

Discussions and Recommendations

Generally speaking, it can be said that the two countries have some legal provisions that can be used to combat identity crime in the real world in cases where identities of the victims are used to create forged documents such as passports, birth certificates and so forth. However, the efficiency of offline laws (laws enacted to deal with real crimes as opposed to crimes occur in computers and the Internet, etc.,) in dealing with the online world (computer crimes, etc.,) where most identity-related crimes take place nowadays can be questioned because these laws were primarily enacted to deal with traditional offences relating to documents and thus they may not easily accommodate crimes in the digital age in which the offenders use sophisticated technology to commit such crimes. From here the paper recommends the two countries to extend the traditional provisions or create new ones that can effectively deal with crimes in the virtual world including identity crime in its different stages.

It is worthy to state here that the legal systems in the two countries are not at the same level of advancement. To be precise, the Malaysian legal system is generally more advanced and up-to-date (Duryana Mohamed , 2012) than its counterpart in Mauritania at least in cyberlaws: "the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e. the Internet" (Animesh Sarmah, at al, 2017). For example, the Malaysian National Cyber Security Agency (NACSA) stated that cyberlaws in Malaysia consist of the Computer Crimes Act 1997, Digital Signature Act 1997, Telemedicine Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, Electronic Government Activities Act 2017, PDPA 2010, Ant-Fake News Act 2018, in addition to Penal Code and Copyright (Amendment) Act 1997 (The NACSA). These laws provide some kinds of protection to different aspects of cyberspace and some of them can be used to combat identity crime as discussed elsewhere in this paper.

In contrast, the Mauritanian legal system can be described as underdeveloped system that still relays on traditional laws to deal with sophisticated matters such as identity crime in the digital world. Despite the above, the Mauritanian legal system includes some cyberlaws such as the Mauritanian Law No. 007-2016 Concerning Cybercrimes and also provisions enacted especially for protecting biogeographic or biometric data related to individuals. Some of those provisions can be found in the Code of Civil Status (Law No. 003-2011). This Code prohibits an unauthorised access to the National Register of Population (NRP) which includes the biogeographic and biometric data related to population of the country and imposes heavy penalties on offenders such as imprisonment for terms from 5 to 10 years and fine from 15 to 30 million of MRO (section 66). Moreover, the Code makes it illegal to copy, publish, delate, modify, etc., such information included in the NRP and punishes such acts by life imprisonment and fine from one hundred and five thousand to two hundred and ten thousand million of the MRO (section 67).

Surprisingly, when the punishment mentioned in the Mauritanian Code compares with its equivalent in the Malaysian Computer Crimes Act 1997, the former seems to be more painful than the later. For example, while the Mauritanian Code uses the term "and" which means both imprisonment and fine are imposed on the offenders, the Malaysian Act uses the phrase, "or" which gives a choice to the courts to choose either imprisonment and fine or one of them. Another manifest of difference can be observed in the penalties themselves. For instance, the Mauritanian Code mentions the minimum and maximum of imprisonment and fine, but the Malaysian Act mentions only the maximum for both. Practically, this means that while Malaysian courts can impose imprisonment for a term of one month, etc., on offenders who unauthorisedly access to computer materials (S 3 CCA), the Mauritanian courts cannot impose imprisonment for a term less than five years in the same crime-unauthorised access to computer materials (s. 66 of Code of Civil Status).

Concluding Remarks

Identity crime in the digital age brings challenges to traditional laws and such challenges should be recognised in order to take proactive reforming steps towards solutions. This paper was dedicated to definition of identity crime, its nature and the capability of current legal systems of Mauritania and Malaysia to efficiently deal with identity-related crimes. In the definition section, the paper found that identity crime in its basic meaning means using identities of others (passports, names, bank accounts, etc.,) to commit crimes under their names or steal their monies and such like. The criminals use many tactics including technological ones such as phishing, hacking, etc., and traditional methods like stealing documents containing the information. Identity crime has many forms (financial and non-financial etc.,) and names such as identity theft, identity fraud and identity crime which is chosen by some to cover all crimes relating to identities.

Regarding the law perspective, identity crime is an old crime that flourishes in the digital age. The existing legal systems in Mauritania and Malaysia have traditional provisions that can be used to deal with types of identity-related crimes and modern provisions that can be useful in combating identity crime in the digital environment. As identity crime is a dangerous crime that could cause damage to individuals, financial organisations and other critical interests, this paper suggested that provisions related to this crime in Malaysia and Mauritania should be updated to efficiently deal with identity crime in its different stages. This can be done either through revising the current laws or enacting special laws for identity crime and crimes occur in the virtual world. The nature and scope of the suggested provisions should be drafted after taking advice of the law enforcement, legal and technological experts and other stakeholders who have a clear picture of the digital world and what is happening on it.

References

Ahmad, S. S. (2007). *Malysian Legal System* (2 ed.). Singapore: LexisNexis.

Animesh Sarmah, at al. (2017, June). A brief study on Cyber Crime and Cyber Law's of India. *IRJET*, p. 1633.

Azmil, S. (1997). Crimes on the Electronic Frontier: Some Thought on the Computer Crimes Acts. *Malaysian Law Journal (MLJ)*, vii.

Duryana Mohamed . (2012). Investigating Cybercrimes Under the Malaysian Cyberlaws and the Criminal Procedure Code: Issues and Challenges. *MLJ, 6*, iv.

Federal Trade Commission. (2019, March 13). *Warning Signs of Identity Theft*. Retrieved from Identity Theft.gov: https://www.identitytheft.gov/warning-signs-of-identity-theft.

Finch, E. (2007). The Problem of Stolen Identity and the Internet. In Y. Jewkes (Ed.), *Online Crime.*

Gercke, M. (2011). Legal Approaches to Criminalize Identity Theft. In UNODC, *Handbook on Identity-related Crime.* New York: United Nations.

IA Pascual, e. a. (2019, March 16). *2018 Identity Fraud: Fraud Enters a New Era of Complexity*. Retrieved 7 30, 2018, from JAVELIN: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

Identity Theft Resource Center (ITRC). (2013). *Identity Theft Resource Center, 2012 Breach List.* Identity Theft Resource Center. Retrieved March 18, 2019, from idtheftcenter.org: https://www.idtheftcenter.org/images/breach/Breach_Report_2012.pdf.

Internet Word Stats. (2019, March 31). *Usage and Population Statistics*. Retrieved May 2, 2019, from Internetworldstats.com: https://www.internetworldstats.com/stats.htm

Jaishankar, K. (2008 , January-June). Identity related Crime in the Cyberspace: Examining Phishing and its impact. *International Journal of Cyber Criminology, 2*(1), 10–15.

Jonathan Stemple , J. (2017, OCTOBER 4). *Yahoo says all three billion accounts hacked in 2013 data theft.* Retrieved March 18, 2019, from REUTERS.

Lawson, P. (2011). Identity-related Crime Victim Issues: A Discussion Paper. In UNODC, *Handbook on Identity-related Crime* (pp. 107-168). New York: United Nations.

Lowyat.net. (2017). *46.2 Million Malaysian Mobile Phone Numbers Leaked From 2014 Data Breach.* Retrieved March 18, 2019, from Lowyat.net: https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from2014-data-breach/.

MACMILLAN English Dictionarry. (2002). Macmillan Publishers Limited.

Malaysia Computer Emergency Response Team (MyCERT). (2018). *MyCERT Incident Statistics.* Retrieved March 19, 2019, from MyCERT: https://www.mycert.org.my/statistics/2018.php.

Milan Jain , P. (2014). Techniques in Detection and Analyzing Malware Executables: A Review. *IJCSMC, 3,* 939-935.

Mohamed, S. M. (2014). Identity Crime in Digital Environment: A Comparative Study Between the Common Law and The Shariah as Applied in Mauritania. *(Unpublished master dissertation, IIUM).*

Mostapha Abd al-Shafi. (2004). *Diwan Imrou Al-Qais* (5 ed.). Beirut: Dar al-Kotob al-Ilmiyah.

Oxford Dictionary of Law (5 ed.). (2003). Oxford University Press.

Oxford Wordpower. (1999). New York: Oxford University Press.

RAO, M. (2018, 4 11). *One in 10 M'sians fall victim to identity theft*. Retrieved May 2, 2019, from themalaysianreserve.com: https://themalaysianreserve.com/2018/04/11/one-in-10-msians-fall-victim-to-identity-theft/

Sarah J. McCarthey , E. (2002, April/May/June). Identity matters. *Reading Research Quarterly, 37*(2), pp. 228–238.

Shun-Yung Kevin Wang , W. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in The Era of the Internet. *Internet Journal of Criminology,* 1-21. doi:ISSN 2045-6743 (Online)

Sidi Mohamed Ould Mohamed, S. (2015, October-November). The Shari'ah Approach to Criminalise Identity Theft. *Pertanika J. Soc. Sci. & Hum. (S), 3*(4/5), 171.

Sunil Kumar , D. (2018). Hacking Attacks, Methods Techniques and Their Protection Measures. *IJSART, 4,* 2253. Retrieved 7 24, 2018, from http://apo.org.au: https://web.archive.org/web/20110501063145/http://www.crimecommission.gov.au/publications/crime-profile-series/_files/identity-crime.pdf

The NACSA. (n.d.). *Malaysian Cyber Laws.* Retrieved March 19, 2019, from NACSA.GOV : https://www.nacsa.gov.my/legal.php.

The Cross-Border Crime Forum. (2019, March 17). *Identity-Related Crime: A Threat Assessment.* Retrieved 07 23, 2018, from Publicsafety.gc.ca : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-dntt-rltd-crm-2010/archivedntt-rltd-crm-2010-eng.pdf.

The International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR). (2011). *Responding to Victims of Identity Crime: A Manual for Law Enforcement Agents.* British Columbia, Canada: The International Centre for Criminal Law Reform andCriminal Justice Policy (ICCLR).

Wall, D. S. (2013). *Future Identities: Changing Identities in the UK- the Next 10 Years.* London: The Crown.

Yahoo. (2016, December 14). *Yahoo Security Notice December 14, 2016*. Retrieved 7 24, 2018, from YAHOO HELP: https://help.yahoo.com/kb/account/previously-announced-company-december-sln27925.html. 23