Master Thesis

E-commerce in the Modern World-Electronic Transactions and Some Challenges and Perspectives: Comparative Analysis of UK, Egypt and South African Legislation

submitted on March 5, 2018

by

Yulia Vladimir Akinfieva

Supervisor

Dr. Richard Oppong
University of Liverpool | Online Programmes

Certificate of Authorship of Thesis

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for an award of any other degree or diploma of a university or other institute of higher learning, except where due acknowledgement is made in the text.

(Signed) Yulia Vladimir Akinfieva

Except as specially indicated in footnotes, quotations and the bibliography, I declare that I am the sole author of the thesis submitted today.

Signature of Author: Yulia Vladimir Akinfieva

Date: 5 March 2018

Abstract

In recent years, the shape and form of global marketplace has been evolving and moving from traditional face-to-face, physical trading practices by means of paper documents, to a more advanced form of trading and transacting through electronic means facilitated by the internet. The trade has evolved and shaped itself to encompass electronic processing and transmission of data, to include text, sound, picture and video formats, and hence, nowadays, by means of the internet and information and communication technologies, businesses can reach consumers who, otherwise, would never had known or had access to certain products and/or services, where commercial transactions became possible between a seller and a buyer who would transact and never meet each other in reality.

The new form of transacting in the global marketplace, coined as electronic commerce has been witnessing tremendous growth and has become the backbone of contemporary economic and financial transactions, as well as the preferred choice for most traders and consumers, offering access not only to national e-stores but wiping the international borders and opening access to cross-border markets.

Rapid growth of global e-space and fast development of technologies and e-commerce, however, have posed significant challenges to the global legal frameworks, and in particular, exposed the limitations of definitions available under the substantive rules applicable to commercial contracts. The more convenient forms of communication and transactions, have confronted governments, internet users and businesses with a wide range of legal issues as the existing legal rules in some jurisdictions, yet, do not provide the answers to novel issues that arise in the course of transactions. Hence, the need for enabling legal frameworks in order to fill the lacuna to instill certainty, confidence and guidance in relation to arising e-commerce matters.

Egypt, which will be the focus of this thesis, is one of those jurisdictions legal framework of which in relation to e-commerce remains underdeveloped and falls way behind legislative instruments of other countries. The regulatory framework in the field of e-commerce in Egypt remains to be yet formulated and enforced as there are still no appropriate laws governing the sector although the Internet Law and E-Commerce Law have long been anticipated. As e-commerce is spreading across borders, Egypt needs Data Protection Law, Online Privacy Law, Consumer Protection, Internet/Cyber Law in order to ensure proper governance and control over rapidly growing electronic market space.

This thesis is intended to explore Egypt's legislative landscape related to e-commerce by analyzing and comparing Egypt's current and proposed legislation to some of the international 'best practices'. The principle jurisdictions identified for the purpose of comparison are the United Kingdom, as an example of advanced jurisdiction and South Africa, as a jurisdiction lying within the same continent.

The thesis is aimed to examine the law(s) regulating e-commerce in Egypt in contrast to international trends and e-commerce laws of the United Kingdom and South Africa. The thesis aims to compare and contrast provisions related to electronic contracts, e-signatures, e-government, aspects of jurisdiction, consumer protection, cybercrime and cryptocurrencies available under Egyptian, UK, and South Africa's legislation. Existing laws and regulations governing e-commerce in South Africa and the UK will be assessed in comparison to Egypt, in order to identify merits of each legal framework which would potentially pave the way for recommendations to be proffered to Egypt's legislators in their attempt to shape the needed regulatory instrument(s).

The thesis covers the dimensions of e-commerce in a legal context as follows: Section 1 deals with the background issues of e-commerce and UNCITRAL and OECD efforts; Section 2 addresses e-commerce legislative landscape of Egypt including E-signature Law, Draft E-commerce Law and challenges associated with electronic contracts; Section 3 examines dimensions of e-commerce in a legal context as available under the laws of South Africa and the United Kingdom and draws analytical conclusions of strengths of the legislations which might serve a lesson from international 'best practice' perspective to be adopted by Egypt's legislators in the course of drafting its own laws; Section 4 discusses cryptocurrencies and its legal status and acceptance in the UK, South Africa and Egypt; and finally, Section 5 presents an analysis of gaps noted and lessons learned from the UK and South Africa and proposals of needed reforms on the legislative landscape of Egypt.

The thesis aims to illustrate that Egypt, is encouraged to consider the experience of other jurisdictions such as the UK and South Africa in the realm of e-commerce related legislative instruments in order to meet the requirements dictated by the new reality, specifically keeping in mind that it has a lucrative market with 100 million (most of which are active users of e-space). Thus, this thesis might very well serve good for the Egyptian legislators looking into modernization of the legal landscape in the field of electronic commerce.

KEYWORDS:

Electronic signature; cyberlaw; e-commerce; electronic contract; consumer protection in electronic transactions; e-government services; E-signature Law of 2004; Egypt Draft Law on E-commerce; cryptocurrencies in Egypt; cryptocurrency in the UK; electronic commerce regulations; advanced electronic signature; electronic communication act; foreign e-signature products and services; the accreditation authority.

Contents

Certificate of Authorship of Thesis 2

Abstract 3

1. Introduction 8

1.1 The Background-Increasing Importance of E-commerce 8

1.2 Challenges Posed by E-commerce to Legal Systems as Compared to Traditional Commerce 10

1.3 UNCITRAL and OECD Efforts 12

1.4 The Problem Defined and The Purpose of the Research 14

The Problem 14

The Purpose 16

2. Electronic Commerce and Electronic Transactions 16

2.1 Egypt's Legislation 16

2.1.1 Egypt's Landscape of E-transactions 16

2.1.2 Egypt's Participation in UNCITRAL and other International Efforts 17

2.1.3 Electronic Signature Law of 2004 19

2.1.4 Draft Law on E-Commerce 21

2.1.5 Electronic Contracts and the Challenge 25

3. Lessons Learned from the E-Commerce Legislation of the South Africa and the United Kingdom 27

3.1 E-Commerce Legislation of South Africa 27

3.1.1 Overview 27

3.1.2 E-signatures 27

3.1.3 Regulation of Foreign E-signature Products and Services 29

3.1.4 E-Signatures in E-Government Services 29

3.1.5 The Accreditation Authority 29

3.1.6 International Electronic Transactions and Jurisdiction 30

3.1.7 Electronic Contract 30

3.1.8 Consumer Protection 31

3.1.9 Cybercrime 32

3.2 Comparison of Legislation (Egypt and South Africa) and Lessons Learned from South Africa's ECTA 33

3.2.1 E-Signatures 33
3.2.2 Regulation of Foreign E-Signature Products 34
3.2.3 E-Signature and E-Government Services 34
3.2.4 Jurisdiction 35
3.2.6 E-Contracts 35
3.2.7 Consumer Protection 35
3.2.8 Cybercrime 36
3.3 E-Commerce Legislation of the UK 36
3.3.1 Introduction 36
3.3.2 E-signatures 38
3.3.3 E-Signature and E-Government Services 40
3.3.4 E-Contracts 40
3.3.5 Consumer Protection 42
3.3.6 Jurisdiction 44
3.3.7 Cybercrime 45
4. The Role of Cryptocurrencies and its Acceptance: Cross-Jurisdictional Approach with Special Emphasis on Egypt 47
4.1 The Status of Cryptocurrencies in Egypt 49
4.2 Current Legal Regulatory Framework in South Africa 54
4.3 The Approach in the UK 56
4.4 Conclusion 57
5. Conclusions and Guidelines for Egypt-Proposals for Reform 58
6. Bibliography 62
6.1 Legislation 62
6.2 Case Law 64
6.3 References 64

List of Abbreviations[1]:

AeS	Advanced Electronic Signature
B2C	Business-to-consumer
CA	Certification Authority (of ITIDA)
CBE	The Central Bank of Egypt
CMA	Computer Misuse Act 1990
CRA	The Consumer Rights Act 2015
E-commerce	Electronic Commerce
EU	European Union
ECA	Electronic Communications Act 2005 (No. 36 of 2005)
ECTA	Electronic Communications and Transactions Act 25 of 2002
FCA	The Financial Conduct Authority
HMRC	Her Majesty Revenue and Customs
IPRs	Intellectual Property Rights
ICT	Information and Communications Technologies
ITIDA	Information Technology Industry Development Authority
LDCs	Least Developed Countries
MLEC	The Model Law on Electronic Commerce
MCIT	Egyptian Ministry for Communications and Information Technology
OECD	Organization for Economic Cooperation and Development
PKI	Public Key Infrastructure
SARB	South African Reserve Bank
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
VCs	Virtual Currencies
WTO	World Trade Organization

[1] The terms are in alphabetical order and not in the order of appearance in text

E-commerce in the Modern World-Electronic Transactions and Some Challenges and Perspectives: Comparative Analysis of UK, Egypt and South African Legislation

1. Introduction

1.1 The Background-Increasing Importance of E-commerce

Commerce in its traditional definition up until late 1990s has been based on the 'physical mode' of operation whereby customers used to conduct trade by means of visiting the physical establishments where transactions of placing their orders, receiving the goods and paying for them took place. The milestone changes to the 'brick-and-mortar' way of transacting has occurred in the late 1990s with the development of internet and its further wide-ranging and far-reaching expansion across the globe which resulted in the development of Electronic Commerce (E-commerce) impacting individuals, business entities and national economies[2]. A paradigm shift has occurred in terms of ways of conducting businesses, where organizations are under pressure from the market forces to do business online and 'develop new e-commerce systems'[3] in order to survive in the highly competitive environment, where consumers have been internalizing the convenience of buying the service/good instantaneously by virtue of a click without having to go anywhere, where new generations will most probably make 'brick-and-mortar' establishments obsolete.

As organizations are striving to compete in the era of electronic commerce, new business models arise, where goods can be delivered by drones to the door-step of the consumer using drone technology, where applications link suppliers with consumers in transportation, food, health, financial and professional services among others via platforms where application provider, the supplier and the consumer can be placed in three different countries[4], where multinational giants such as General Electric (GE) do not only sell equipment but rather services by selling 'equipment that have remote-monitoring capabilities that allow GE to monitor and operate them'[5]. Developments in the information and communication technologies (ICTs) had led e-commerce to grow

[2] B H. Malkawi, 'E-commerce in Light of International Trade Agreements: The WTO and the United Sstates-Jordan Free Agreement', (Summer 2007), *International Journal of Law and Information Technology*

[3] S C Henderson, 'Is Auditor Participation in Developing Electronic Commerce Systems: The impact on System Success' (2002) Ph.D. Thesis, Auburn University, Australia.

[4] 'The WTO's Discussions On Electronic Commerce' (2017) Analytical Note SC/AN/TDP/2017/2 retrieved 17 September 2017 from http://www.intgovforum.org/multilingual/sites/default/files/webform/AN_TDP_2017_2_The-WTO%E2%80%99s-Discussions-on-Electronic-Commerce_EN.pdf

[5] R Atkinson, 'Testimony before the Committee of Ways and Means Trade Subcommittee, Hearing on 'Expanding US Digital Trade and Eliminating Barriers to Digital Exports' (2016), July 13, retrieved 15 September 2017 from http://waysandmeans.house.gov/event/hearing-expanding-u-s-digital-trade-eliminating-barriers-u-s-digitalexports/

'from being an early 90's fascination into giving brick and mortar retailers a real run for their money'[6]. Being on the edge of the 'new technology frontier'[7], standing at the entrance gate of the 5G era, data becomes the new currency of the digital economy, where data is analyzed and becomes the critical factor of the competitive advantage, new business models will yet arise. Meanwhile, the scope of the recent 'electronic phenomena' is truly impressive, according to a recent Forbes report it is estimated that the e-commerce industry will surpass USD 2 trillion annual haul in 2017[8], a yet bolder forecast is USD 4 trillion in retail e-commerce sales by 2020[9]. Further, IBM analyst reveals that about 71% of consumers are 'showrooming' and 'webrooming' in an attempt to find the best price[10]. The growth rate of e-commerce is exponential as illustrated by the US Census Bureau[11] with 0.5% annual growth for the fiscal year of 2015, and a ten-fold increased rate between 2015 and 2017, and an expected ten-fold or more increase between 2017 and 2020[12].

E-commerce being a new model and paradigm exponentially growing and embracing the globe, obviously requires re-assessment and adaptation of internal business models of organizations, as well as external frameworks such as tax, regulatory, risk and compliance frameworks, trade and consumer protection environments which obviously were tailored to serve the older business models and are not equipped enough to meet the challenges posed by the new digital reality.

In the traditional era of the business models, organizations might have taken long years prior to becoming global players. During these years as establishing their presence in jurisdictions where they conducted business, they had time and opportunity to learn the rules and laws of those countries. Nowadays, however, organizations conducting business on the internet is by definition a global player. Consequentially, it is becoming more challenging in terms of learning rules and regulations of different jurisdictions prior to becoming subject to them[13], or considering consequences of entering jurisdictions which do not have proper legislation in place regulating electronic commerce.

As E-commerce is affecting wide array of sectors of the community including but not limited to governments, professional organizations, financial institutions, services and goods providers, educational institutions, infrastructure providers and technology consultants, multiple contingent issues arise.

---

[6] M Lazar, 'E-commerce Statistics and Technology Trendsetters for 2017' (March 4, 2017), IBM official website accessed 10 September 2017 at https://www.ibm.com/developerworks/community/blogs/d27b1c65-986e-4a4f-a491-5e8eb23980be/entry/Ecommerce_Statistics_Technology_Trendsetters_for_20171?lang=en

[7] Ibid (3)

[8] Ibid (5)

[9] ibid

[10] ibid

[11] https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf?cm_mc_uid=80910170544715056493721&cm_mc_sid_50200000=1505649372

[12] Ibid (5)

[13] F Sudweeks, C.T. Romm, 'Introduction' In *Doing Business on the Internet: Opportunities and Pitfalls*, (London: Springer-Verlag: 1-7, 1999)

1.2 Challenges Posed by E-commerce to Legal Systems as Compared to Traditional Commerce

Indeed, it is not only that ICTs have triggered the creation of new business models for implementing transactions but rather these technologies have 'fundamentally changed the character of many commercial and other relationships'[14]. As one author described the effect of ICTs on law[15]:

> *[A] new system of communication does more than make us more knowledgeable or our institutions more efficient. It also leads to the creation of new relationships and, most importantly, changes our attitudes, expectations, and ways of thinking about law.*

In American commercial legislation, for example, commercial law has been described as 'legislation which is designed to clarify the law about business transactions rather than to change the habits of the business community' and the principal objective of the drafters of commercial legislation is 'to be accurate and not to be original'[16]. However, according to Nimmer[17] this has not been the approach in legislation related to e-commerce. What has been witnessed is the creation of new law, 'often regulatory in nature'[18] and that is due to the assumption that regulations governing traditional commerce 'inadequately safeguard consumer or other protected interests'[19]. Furthermore, it is believed by some that escalated 'risks of abuse in e-commerce'[20] exist that call for 'proactive regulation'[21] which provides for safeguards even prior to the occurrence of actual abuse. Given the nature and speed of e-commerce expansion and penetration, an enormous expansion of the 'new law' is witnessed[22] which brings around an array of new regulations, conflicting at times, or which 'represent a grab for control than sound legal or social policy'[23]. And these developments are being dealt with by not only legislators but by consumers and trading companies which must adapt to the new legal systems.

Robust development of e-commerce and technical specificity associated with such online transactions have posed several challenges to the traditional legal system governing traditional commercial relationships, among which are four major categories as noted by K C Lauden and C G Traver[24], which are issues associated with information rights, property rights, governance, public safety and welfare.

---

[14] R T Nimmer, 'The Legal Landscape of E-Commerce: Redefining Contract Law in an Information Era' (2006) A paper presented at the Journal of Contract Law Conference, 'Contract and the Commercialisation of Intellectual Property', presented by the Singapore Academy of Law and Singapore Management University, September 2006

[15] M Ethan Katsh, *The Electronic Media and the Transformation of Law* (University of Massachusetts Press, Boston, 1989), 22.

[16] G Gilmore, 'On the Difficulties of Codifying Commercial Law' (1948) 57 *Yale LJ* 1341.

[17] Ibid (14)

[18] ibid

[19] ibid

[20] ibid

[21] ibid

[22] ibid

[23] ibid

[24] K C Lauden, C G Travor, *E-Commerce: Business, Technology, Society* (Pearson/Addison Wesley, 2004)

Consider, for example, contracts, an essential element of any commercial transaction, in the context of e-commerce, an offer, an acceptance and consideration will yet be valid and applicable, however, given the new nature of means of communication (e-mails, online transactions on the website etc.) raises an issue of the exact time of acceptance, and hence, calls for regulation as to when and how the acceptance took place[25]. Online identity in respect to the capacity to enter into a commercial relationship, legitimacy is another aspect which calls for specific regulation unavailable in traditional systems, and here one of the methods introduced and dealt with is the electronic signature[26].

Among the first policy challenges associated with e-commerce to surface was the matter of privacy and data protection[27] whereby ICTs and their embedded security loops in the system makes it easy for websites to gather private information about consumers, and hence, dissemination of sensitive information, sending spam mails, tracking of activities of consumers[28] among others all become real threats and concern of consumers, both natural and juristic persons.

Another challenge lies in the field of intellectual property rights protection. Cyberspace being a boundless medium, raises serious concerns to organizations with regards to protection of their IPRs as traditional laws protecting such rights in the 'physical world'[29] might not be effective in protecting those rights in the virtual reality. Issues in this respect can arise in determining subject-matter of protection, ascertaining novelty and originality, enforcement of IP rights, preventing unauthorized hyper-linking and meta-tagging (note, these concepts are not available in the traditional legislation and are highly technical), as well as in protection against unfair competition[30].

Contract related associated issues, data privacy and protection of IPR are some of the challenges associated with the e-commerce. The robust spread of digital economy, does provide businesses access to customers across borders as well as offers a wide space for consumers to shop, choose, access prices and suppliers, and lower costs of transactions. However, despite the advantages the new model of economic transactions offers, the businesses, consumers and legislators, all have valid concerns as to what laws and regulations shall govern electronic transactions. The question arises as to jurisdiction and conflicts of law[31], where traditional rules of private international law, stipulate that the jurisdiction extends to those within the country or to transactions taking place within the borders of that jurisdiction[32].

---

[25] K S Barath, V Mahalkshmi, 'Legal Issues in E-Commerce Transactions- An Indian Perspective' (2016) Vol 4 Issue 11 *International Journal on Recent and Innovation Trends in Computing and Communication* 184-191

[26] ibid

[27] R Bone, 'The Challenges of Law in Cyberspace-Fostering the Growth and Safety of E-Commerce' Commissioner Mozelle W. Thompson, Federal Trade Commission accessed 30 September 2017 at http://www.bu.edu/law/journals-archive/scitech/volume6/presentation.pdf

[28] Ibid (26)

[29] ibid

[30] ibid

[31] Ibid (28)

[32] Ibid (26)

However, organizations which access consumers across the globe, and vice versa, would mean that they might become subject to laws of every jurisdiction which in turn differ significantly and in particular in relation to 'comparative advertising, advertising to children, rights of withdrawal from contracts, the 'cooling off' rules'[33] etc. Therefore, the matter becomes that of predictability and compliance for businesses, and convenience and protection under the jurisdiction of consumers' domicile laws and regulations.

Another important aspect which poses a challenge to the traditional legal systems and arose with the development of digital economy is the necessitation of the evolution of electronic payment methods, to e-finance instruments and cryptocurrencies which are now commonly used for the electronic transactions over the internet. Therefore, regulation of such instruments became an essential requirement which shall address such issues as secure credit card transactions, determination of competent jurisdiction, recognition of cryptocurrencies, consumer-oriented risk among others[34].

As is evidenced, the legal systems of countries across the globe have been trying to cope with the emerging issues and challenges posed by the newly evolved digital marketplace, addressing challenges associated with data privacy, conflicts of law, contracts and lack of regulations in some countries. Efforts of some jurisdictions as well as UNCITRAL, are of special significance to look at in the context of this dissertation work.

1.3 UNCITRAL and OECD Efforts

UNCITRAL

In 1996, the UNCITRAL released the UNCITRAL Law on Electronic Commerce[35] along with the Guide to Enactment, which is to provide the background and explanatory information to enable States to prepare the needed legislative provisions in this regard[36]. The UNCITRAL Model Law primarily deals with the legal recognition of data messages, electronic contracts but does not cover consumer protection. The UNCITRAL Law is applicable to 'any kind of information in the form of a data message used in the context of commercial activities'[37]. The objective of the law was two-fold: 1. To provide national legislators with a set of international rules for establishing a secure legal environment for e-commerce for facilitation of its applicability and utilization; and, 2. To facilitate equal treatment for 'users of paper-based documentation and to users of computer-based information'[38], recognized as 'functional-equivalent approach'[39]. Apart from formulation

[33] Ibid (28)
[34] Ibid (26)
[35] UNCITRAL Model Law on Electronic Commerce with Guide Enactment 1996 with additional article 5 bis as adopted in 1998 accessed 8 October 2017 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[36] UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998 accessed 8 October 2017 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[37] Ibid (37) Article 1
[38] See 'Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)', contained in Model Law (Objectives No. 5)
[39] Article 5 of the Model Law states: 'Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.'

of the legal notions of 'non-discrimination, technological neutrality and functional equivalence'[40], the MELC has established rules for the 'formation and validity of contracts'[41] transacted by electronic means, for the 'attribution of data messages', for the 'acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages'[42]. Further, certain provisions of the MLEC have been amended by the Electronic Communications Convention[43] given the developments in e-commerce activity. Furthermore, Part II of the MELC, has been complemented by the United Nations Convention of Contracts for the International Carriage of Goods Wholly or Partly by Sea[44] (the 'Rotterdam Rules') as well as other legal texts. These rules aimed at providing guidance and legal framework taking into consideration technological developments which happened in the maritime transport including but not limited to the growth of 'containerization'[45], door-to-door carriage under a single contract, and the advance of e-transport documents[46].

OECD

Other significant efforts in the realm of electronic commerce have been undertaken by the Organization for Economic Cooperation and Development (OECD), which placed e-commerce as a central element of its vision for 'economic growth, jobs and improved social conditions'[47]. OECD activities have been centered along the following lines: 1. Building trust for users and consumers; 2. Establishing ground rules for the digital marketplace; 3. Enhancing the information infrastructure for e-commerce; 4. Increasing the benefits of e-commerce[48]. OECD's efforts touched upon such important aspects of e-commerce as privacy, authentication, consumer protection, tax related matters, infrastructure among others. OECD has been active since 1990s exploring policy and regulatory matters, promoting information flow between public and private sectors in relation to ITCs developments and in particular electronic authentication and certification issues[49]. OECD has delivered several important efforts and papers with regards to e-commerce among which are Guidelines on the Security of Information Systems (1992)

[40] Ibid (36)
[41] ibid
[42] ibid
[43] United Nations Convention on the Use of Electronic Communications in International Contracts accessed 8 October 2017 at http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf
[44] United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (New York, 2008) (the "Rotterdam Rules") http://www.uncitral.org/uncitral/en/uncitral_texts/transport_goods/2008rotterdam_rules.html
[45] ibid
[46] ibid
[47] OECD MINISTERIAL CONFERENCE "A BORDERLESS WORLD: REALISING THE POTENTIAL OF GLOBAL ELECTRONIC COMMERCE OTTAWA, 7-9 OCTOBER 1998 OECD ACTION PLAN FOR ELECTRONIC COMMERCE SG/EC(98)9/FINAL accessed 8 October 2017 at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En
[48] ibid
[49] ibid

and on Cryptography Policy (1997)[50]. Further, the Ministerial Declaration on Authentication for Electronic Commerce had recognized the significance of authentication in e-commerce and put forward certain elements of development in this field. Efforts of OECD in this regard have been focusing on improving consumer confidence in e-commerce and enabling the development of 'the global marketplace'[51], in specific, enhancing consumer protection by addressing such matters as disclosure of sensitive information, handling of complaints, dispute resolution, and advertising among others[52]. Moreover, the OECD Action Plan for Electronic Commerce[53] has emphasized the significance of OECD efforts in relation to authentication and privacy matters, consumer protection and tax issues. On the other hand, the Guidelines for Consumer Protection in the Context of Electronic Commerce[54] deal with business-to-consumer matters.

The Guidelines developed by the OECD in its efforts to address the challenges posed by e-commerce are 'technology-neutral' aimed at enabling initiatives of the private sector and focusing on the necessity for collaboration between states, organizations and consumers[55] with specific objectives of instilling fairness in business transactions, clarity in terms of information about 'online business's identity'[56], transparency of transactions' process, fairness and affordability of dispute resolution mechanisms as well as protection of privacy.

1.4 The Problem Defined and The Purpose of the Research

The Problem

Rapid growth of global e-space and fast development of technologies and e-commerce, have posed significant challenges to the legal framework, and in particular, exposed the limitations of definitions available under laws of different countries as evidenced in various efforts on the international arena including but not limited to those undertaken by UNCITRAL and OECD, as well as individual governments. Keeping up with such rapid developments in ICTs is challenging for the developed countries and international

[50] ibid
[51] ibid
[52] ibid
[53] The OECD Action Plan for Electronic Commerce was endorsed by Ministers at the OECD Ministerial Conference, "A Borderless World: Realising the Potential of Global Electronic Commerce", held on 7-9 October 1998 in Ottawa, Canada; available at http://www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)9-final.
[54] The Guidelines for Consumer Protection in the Context of Electronic Commerce, approved on 9 December 1999 by the OECD Council, available at www.oecd.org.
[55] H Huffmann, 'Consumer Protection in E-Commerce: An Examination and Comparison of the Regulations in the European Union, Germany and South Africa that Have to Be Met in Order to Run Internet Services and in Particular Online Shops' (2004) LL.M Thesis, University of Cape Town accessed 10 October 2017 at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.7671&rep=rep1&type=pdf
[56] ibid

organizations, not to mention developing countries for which ICTs present an increasing concern. There is now unquestioned evidence that businesses gain substantially from e-commerce and widespread application of ICTs have led to significant growth in productivity in industrialized countries leading to creation of 'millions of new jobs and billions of dollars in savings'[57]. However, one of the issues is that figures on e-commerce and application of ICTs do not exist for developing countries and the only statistical indicators available are those related to internet usage[58]. Although these figures are important, as internet usage is a 'prerequisite for e-commerce'[59] they are not indicative of e-commerce participation. Furthermore, developing countries and especially the least developed countries (LDCs) are ill-equipped or unequipped at all to deal with the challenges and opportunities emerging from 'digitalization'[60]. Therefore, many of those LDCs, specifically those with low level of readiness for engagement in e-commerce and with limited experience in the field, are in an urgent need of formulation of policies and laws applicable to the digital economy, given also that many developing countries lack 'legislation in this area altogether'[61].

Egypt, which is the primary focus of this paper is one of those developing countries that lacks legal framework which would properly address the issues of the digital economy. Egypt is in an urgent need to formulate proper laws in order to keep pace with the developments on the arena of e-commerce, new developments in technology and the manner in which the modern trade happens. Over the past decade, the Egyptian government has undertaken a number of initiatives to meet the realities and needs of the newly emerged e-commerce including establishment of the Internet Society in Egypt in 1997, issuance of Ministerial Decree No. 2 of 1999[62], formulation of the national telecommunications and information technology plan (January, 2000)[63] as well as formulation and enforcement of Electronic Signature Law[64] in 2004. However, these initiatives remain 'short of providing an efficient institutional infrastructure capable of handling the promotion, governance and diffusion of electronic commerce'[65].

In this context, instead of re-inventing the wheel, this paper aims to explore experiences, with their benefits and challenges, of other more developed

[57] 'ICT and E-Commerce-An Opportunity for Developing Countries' (2003) United Nations Conference on Trade and Development. Issues In Brief No. 1
[58] Ibid
[59] ibid
[60] 'Information Economy Report: Digitalization, Trade and Development' (2017) UNCTAD Overview accessed 15 October 2017 at http://unctad.org/en/PublicationsLibrary/ier2017_overview_en.pdf
[61] ibid
[62] Ministerial Decree No. 2 of 1999 issued by the Ministry of Trade and Supply to formulate a committee to develop the electronic commerce legislation
[63] M Brown, 'Advancing E-commerce in Egypt: Legal and Regulatory Recommendations' (2000) report submitted to the Ministers of Economy and Foreign Trade and Communication and Information Technology
[64] Law 15 of 2004 on E-Signature
[65] S Kamel, A Ghoneim, S Ghoneim, 'The Impact of the Role of the Government of Egypt on Electronic Commerce Development and Growth' (2004) Chapter XII, Idea Group Publications, USA accessed 19 April 2017 at https://www.academia.edu/7884704/The_Impact_of_the_Role_of_the_Government_of_Egypt_in_Electronic_Commerce_Development_and_Growth

jurisdictions, lessons of which Egypt can absorb, and, in specific, the paper will examine and compare legislation of the UK as being the representative of a developed nation and laws of South Africa, jurisdiction located on the same continent as Egypt.

The Purpose

Research that addresses current regulations and initiatives of Egypt in the field of e-commerce is scarce, and hence, needs further attention. The primary objectives of this paper, are therefore, to: 1. Analyze the current state of legislation in Egypt addressing e-commerce issues; 2. Compare Egypt's initiatives with this regards with developments in the UK and South Africa.

2. Electronic Commerce and Electronic Transactions

2.1 Egypt's Legislation

2.1.1 Egypt's Landscape of E-transactions

Egypt's government has been investing in the infrastructure of communication and information technology since 1985[66]. In 2008 one million of the population had access to broadband internet, and only 8.62 million of the eighty-three million population (approximately 10%) were internet users[67]. In 2017, according to the report by the Ministry of Communication and Information Technology of Egypt, internet users increased by 7 million within one year reaching a 33.19 million[68] mark in April 2017 (with the population of Egypt marking approximately 98 million as of October 2017). ADSL subscribers increased to 4.57 million as of April 2017 compared to 4.05 million of the same month of 2016, mobile data users have jumped to 33.22% in 2017 as compared to 27.37% in 2016[69]. Despite the rapid growth of internet users base, business-to-consumer (B2C) digital trade has been hindered by such factors as preference granted to cash as opposed to credit cards[70], security issues[71], cultural pre-disposition to bargaining the purchase price, poor design and

[66] S Kamel & M Hussein, 'The Emergence of E-Commerce in a Developing Nation: Case of Egypt', *(2002)* 9:2 *BENCHMARKING: AN INTERNATIONAL JOURNAL 146,* 146-53 *, available at* http://www.emeraldinsight.com/Insight/viewContentItem.dojsessionid=07E05F64F61893COAFB15728FB88F6F3?contentType=Article&contentId=843047. an analysis of Egypt's communications infrastructure, see *National Profile for the Information Society in Egypt,* U.N. ECON. & Soc. COMM. FOR W. ASIA (2005), *available at* http://www.escwa.un.org /wsis/reports/docs/Egypt_2005-E.pdf

[67] S E Blythe, 'E-commerce Security in the Land of the Pharaohs: Refining Egypt's Electronic Signature Law' (2011) 21 *Ind. Int'l & Comp. L. Rev.* 181

[68] 'Internet users in Egypt hit 33M in April 2017' Egypt Today, August 21, 2017 accessed 15 October 2017 at https://www.egypttoday.com/Article/1/18486/Internet-users-in-Egypt-hit-33M-in-April-2017

[69] ibid

[70] I Elbeltagi, *'E-Commerce and Globalization: An Exploratory Study of Egypt' (2007),* 14:3 *CROSS-CULTURAL MGMT: AN INT'L J.,* 196, 196-201

[71] J H Abawaji, *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications* (IGI Global, 2012)

security of websites and 'inconsistent return policies' by online traders[72]. On the other hand, business-to-business e-commerce has been growing[73].

According to Blythe[74] one of the aspects of the growing e-commerce in Egypt 'is the cost-plus based market for electronic signatures'[75] where the market for electronic signatures is competitive and the market size is small. Hence, the potential of growth is high which has led private entities to outsource e-signature related services for financial and other operations[76]. Moreover, governmental units including public utilities have 'adopted public key infrastructure services'[77] resulting in significant growth of demand for PKI and electronic signature systems.

2.1.2 Egypt's Participation in UNCITRAL and other International Efforts

Egypt, in preparation stage of drafting of the E-signature law, issued a Decree No. 209 of the year 2000[78] which formed a Committee[79] consisting of representatives from the Ministry of Justice, Ministry of Finance, Ministry of Interior, Ministry of Foreign Affairs, as well as the Ministry of Economy and Foreign Trade, the Ministry of State for Administrative Development. The Committee was also joined by Egypt's Central Bank and the Cabinet Information and Decision Support center along with experts from private sector and academia[80]. The objective of the created Committee was to work on the draft of the E-signature Law taking into consideration experiences of other jurisdictions and international organizations including but not limited to drafts of e-signature and e-commerce laws passed by the UNCITRAL, the

---

[72] 'Introduction to E-Commerce', LINKEGYPT, http://www.linkegypt.com/blogs/b/Introduction-to-ecommerce/22/Introduction-to-ecommerce.html (last visited Apr. 2, 2011)

[73] Economist Intelligence Unit, *Egypt: Overview ofE-Commerce,* GLOBAL TECH. F. (Aug. 3, 2007), http://globaltechforum.eiu.com/index.asp?layout=printer-friendly&doc-id=11174.

[74] Ibid (68)

[75] ibid

[76] ibid

[77] Ibid (A public key infrastructure (PKI) allows users of the Internet and other public networks to engage in secure communication, data exchange and money exchange. This is done through public and private cryptographic key pairs provided by a certificate authority. As defined by Technopedia accessed 22 October 2017 at https://www.techopedia.com/definition/4071/public-key-infrastructure-pki;

PKI consists of four steps:

1. The first step in utilizing PKI is to create a public-private key pair. The private key will be kept in confidence by the sender, but the public key will be available online.
2. The second step is for the sender to digitally sign the message by creating a unique digest of the message and encrypting it. A hash value is created by applying a hash function-a standard mathematical function-to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Once processed, the hash function is encrypted, or scrambled, by the signatory using his private key. The encrypted hash function is the digital signature for the document.
3. Once encrypted, the sender attaches the digital signature to the message and sends both to the recipient.
4. Finally, the recipient decrypts the digital signature by using the sender's public key. If decryption is possible, the recipient knows the message is authentic, that it came from the purported sender. Finally, the recipient will create "a second message digest of the communication and compare it to the decrypted message digest. If they match, the recipient knows the message has not been altered."

[78] Decree No. 209 of the year 2000 of the Minister of Communications and Information Technology

[79] See http://isdo-hwahab/isdo/Esignature.asp and also http://www.mcit.gov.eg/proj_link.asp, last visited on 28 June 2004.

[80] Judge E Elsonbaty, 'The Electronic Signature Law: Between Creating the Future and the Future of Creation' (2005) *Digital Evidence and Electronic Signature Law Review* www.deaeslr.org

US, the EU, France, Ireland, Malaysia and other nations implementing the same. Many countries[81] at the time of drafting of Egypt's E-signature Law have followed recommendations of UNCITRAL and its Model E-Commerce Law passed in 1996. However, Egypt was far from implementing all the recommendations and adapting all experiences it considered in the process of drafting of its E-signature Law[82]. Defining the E-signature and E-writing in Article 1[83]and granting the newly established entity (the Information Technology Industry Development Authority (ITIDA) wide powers[84] did not mean regulation of e-commerce and its various fields as was meant by the model law prepared by UNCITRAL.

On the other hand, apart from UNCITRAL, Egypt in its efforts to participate in legislation efforts related to global e-commerce has concluded a bilateral statement with the United States (1999) with the purpose of aligning with the aims of the US to 'establish a common agreement with trading partners on basic US policy positions and principles[85] concerning the evolving global governance and development of the Internet'[86].

More recent developments and participation of Egypt have been witnessed in March of 2017 when the new national e-commerce strategy developed by the United Nations Conference on Trade and Development (UNCTAD) in collaboration with the Egyptian Ministry for Communications and Information Technology (MCIT) has been presented. The strategy was developed based on the request from the Government of Egypt and has been developed based on the contributions resulting from partnership with the World Bank on e-payments, International Labor Organization, International Trade Center, Organization for Economic Cooperation and Development (OECD) as well as European Commission[87] tackling such aspects

[81] European Union (1999), the United Kingdom (2000), Hong Kong (2000), Spain (2002), Jordan (2001), Tunis (2000) among others.

[82] Articles 16, 17 and 28 of Law No.15/2004 were adopted from UNCTIRAL model law (https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf)

[83] Law No. 15/2004 on E-Signature and Establishment of the Information Technology Industry Development Authority (ITIDA) Article 1 (a)(c)

[84] Ibid Article 4

[85] As provided in the U.S.-U.K. Joint Statement, the provisions typically proclaim general principles that are the cornerstone of U.S. policy on global e-commerce. For example: • The private sector should lead in the development of electronic commerce and in establishing business practices. • Governments should ensure that business enjoys a clear, consistent and predictable legal environment to enable it to prosper, while avoiding unnecessary regulations or restrictions on electronic commerce. • Governments should encourage the private sector to meet public interest goals through codes of conduct, model contracts, guidelines, and enforcement mechanisms developed by the private sector. • Government actions, when needed, should be transparent, minimal, non-discriminatory, and predictable to the private sector. • Cooperation among all countries, from all regions of the world and all levels of development, will assist in the construction of a seamless environment for electronic commerce. (adopted from see ibid(86)

[86] S S Malawer, 'Global Governance of E-Commerce and Internet Trade: Recent Developments (2001) Features: International Law Section accessed 29 October 2017 at http://www.worldtradelaw.net/articles/malawerecommerce.pdf.download

[87] 'Egypt Poised to Accelerate E-commerce Growth with New National Strategy' (20 March 2017) accessed 29 October 2017 at http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1453

as legal and regulatory environment, electronic payments, e-procurement, ICT infrastructure and telecom services etc.[88]

2.1.3 Electronic Signature Law of 2004

Establishment of the Information Technology Industry Development Authority (ITIDA)

The Electronic Signature Law No. 15 of Egypt has been enacted in 2004 introducing the concept of electronic signature and establishing a public authority (ITIDA) with granted public corporate personality and affiliated with the Ministry of Communications and Information[89].

Goals, Objectives and Authorities

The objectives of the established entity are set forth in Article 3 of the Law among which are: 'a) Encouraging and developing information and communications technology; b) Transferring and using advanced information technology; c) Increasing opportunities for exporting communications and information technology services and the products thereof; d) Participating in the development and improvement of entities operating in the ICT field; e) Promoting and supporting small and medium enterprises (SMEs) in the area of using and applying the electronic transaction mechanisms (applications); f) Regulating the activities of e-signature services and other activities in relation to e-transactions and the information technology industry'[90].

ITIDA is granted the power to establish technical standards for electronic signatures[91] whereby regulating these standards it issues certification of authority licenses (CA) to applicants that meet qualifications[92]. The Authority is also authorized to run audits of CAs and identify the services qualified enough to perform. It is entrusted with dispute settlement mechanism and authority to settle customer complaints with regards to CA

[88] The strategy outlines strategic recommendations to tackle challenges and bottlenecks identified through a diagnostic of Egypt's e-commerce landscape on the basis of an integrated framework of policy areas of strategic importance to e-commerce development. The strategy covers ICT infrastructure and telecom services; logistics and trade facilitation; legal and regulatory environment; electronic payments; skills development and building talent; and e-procurement.
[89] Law No. 15/2004, Article 2
[90] Ibid Article 3
[91] Ibid (68)
[92] Ibid (law 15/2004) Article 4

services serving as a board. The Board is also responsible for provisions of technical advice related to disputes between CAs, subscribers and third parties[93].

Moreover, ITIDA offers technical and training consultations for the firms operating in IT sector and their employees, it supports developers of softwares as well as promotes IT trade fairs and events.

The New Form of 'Writing' and 'Signature' Requirement

Egypt's E-Signature Law notable as it is one of the few legislative pieces in the world that 'does not contain exclusions'[94]. The law basically grants e-signatures and 'information written electronically or digitally'[95] the same legality in civil, commercial and administrative matters as ink signatures and documents as recognized under the Evidence Law[96]. Accordingly, legal validity of the electronic form in documents related to wills, marriage and divorce, contracts, deeds in real estate and other transactions is recognized, which is creditable and is supposed to facilitate acceptance of electronic form in wide spectrum of matters. However, in practice, the Law would cover all transactions written and signed electronically only if they are executed in accordance with the provisions of the Law and its Executive Regulation[97]. Moreover, if the law stipulates that 'an ink signature must be executed on a paper document to incur a legal right in a transaction, that requirement is deemed to be met with the attachment of a secure e-signature to an electronic document'[98]. Pertinent to Article 18, for the e-signature to be acceptable as evidence, it shall comply with the following:

A. The e-signature is for the signer solely
B. The signer has sole control over the electronic medium
C. Possible discovery of any modification or replacement of the data of electronically written message or e-signature.

[93] Ibid (68); ibid (law 15/2004)
[94] Ibid (68) 14
[95] Ibid (81) 47
[96] Article 14: Within the scope of civil, commercial and administrative transactions, e-signatures shall have the same determinative effect that signatures have under the provisions of the Evidence Law in the civil and commercial articles, if the creation and completion thereof come in compliance with the terms stipulated in this Law and the technical and technological rules identified in the Executive Regulations of this law.
Article 15: Within the scope of civil, commercial and administrative transactions, e-writing and electronically written messages shall have the same determinative effect that writing, official, and unofficial messages have under the provisions of the Evidence Law in the civil and commercial articles as long as it meets the terms and regulations stipulated in this Law in compliance with the technical and technological rules identified in the Executive Regulations thereof.
Article 16: The hardcopy of the electronically written message shall have the same determinative effect on all parties to the extent that this hardcopy is conforming to the original electronically written message, and as long as the official electronically written message and the e-signature are saved on an electronic backup archiving.
Article 17: Unless stipulated in this Law or the Executive Regulations thereof, the provisions of the Evidence Law in the civil and commercial articles shall prevail in relation to proving the validity of the official and unofficial electronically written messages, e-signatures and e-writings.
[97] Article 14
[98] Ibid (68); Article 17; to be noted that The Evidence Law requirements override the provisions of the E-signature Law in determining the validity of e-documents and e-signatures.

The Executive Regulations of this Law shall set out the necessary technical and technological rules[99].

One of the flaws herein is that the Executive Regulation of the Law 15/2004[100] while setting the implementation grounds, deals with one form of e-signature which is the encrypted signature supported by certificate. Therefore, the Law does not provide for acceptance of other forms of e-signatures even provided that they satisfy provisions of Articles 15, 16 and 17 of the E-Signature Law (adopted from the UNCITRAL Model Law).

Digital Certificates and Certification Authorities

E-signature Law as well as its Executive Regulation provides for the necessary protection and governance by obligating all entities offering services of electronic verification and services related to e-signatures to obtain licenses (Articles 19-27). Noteworthy, that the law has granted absolute control to the Regulator with regards to all aspects of licensing including procedures, fees, issuance and privacy.

A digital certificate serves the purpose of identification of the 'holder of a private key' which is used to create an e-signature[101]. Such digital certificates can only be issued by licensed Certification Authorities and only after information of subscribers has been verified[102]. ITIDA grants licenses only to those meeting qualifications and settling the registration fees[103], with the validity period granted for the license determined by the Board and not exceeding ninety-nine years[104]. Once the license is obtained the Cas are not permitted to 'cease their activities, merge with another firm or waive their license with respect to a third party' prior written consent of ITIDA[105].

Unlike other countries it is evident that Egyptian legislation does not encourage unlimited number of Certification Authorities by imposing very rigid regulations and compliance qualifiers.

2.1.4 Draft Law on E-Commerce

[99] Article 18
[100] Decree No. 109 of the year 2005 issuing Executive Regulation of E-Signature Law No. 15/2004
[101] Ibid (Article 20 contains description of the data to be contained in the digital certificates)
[102] Articles 27, 21
[103] Article 19 of the E-Signature Law; Cas are selected 'under public competition' and the 'fees to be identified by the Authority's Board of Directors'
[104] ibid
[105] Ibid (68); Articles 23, 26 of the E-Signature Law

Most of the more advanced legal systems followed and adopted main pillars as set forth by the UNCITRAL in its Model E-Commerce Law of 1996, EU in 1999, UK in 2000, Hong Kong (2000), Spain, Jordan, and Tunis among others. Egypt, however, is way behind with its draft law on E-commerce proposed back in 2001 and, yet unratified as of now in 2018.

Egypt's E-Commerce Draft Law, covers issues related to e-documents, e-signature, authentication and encryption, consumer protection and fraud, privacy, taxes and tariffs as well as dispute settlement[106]. In Article 1, the relevant terms are defined: e-commerce, electronic deed, electronic contract, e-signature and electronic fulfillment, authority of electronic signature attestation, encryption and domain names[107].

Similar to E-Signature Law, E-Commerce Draft Law grants wide powers to the responsible Minister, which on one hand, makes the law flexible whereas simultaneously increases uncertainty by 'making the rules subject to continuous change and vulnerable to pressures from different interest groups'[108].

Privacy is one of the important aspects regulated by the proposed law, given the fact that Egypt's law is quite restrictive in relation to privacy violations. As for example, customer's bank information cannot be exchanged between banks or released elsewise without the consent of the customer[109]. Therefore, legislation addressing privacy must be carefully tailored incorporating main principles of the Egyptian laws as well as considering potential conflicts with national security concerns and international laws. The current draft addresses privacy in such a way as to preserve the abovementioned considerations. E-commerce Draft Law does not address authentication matters which is dealt with by the E-Signature Law, however, the draft suggests that there shall be a number of Certification Authorities although no specific Authority in this regard was identified. Furthermore, the draft law deals with encryption, however, it references all of particularities in relation to the Executive Regulation which has not been issued. The only exception is that the draft law explicitly identifies the governmental third party which shall be responsible for archiving the encryption keys[110] and suggests that privacy in alignment with main principles of Egyptian law is preserved in Article 9:

'The encrypted data is considered to be personal and cannot be revealed or duplicated without written approval from the concerned person, or by a judicial order. The code is considered as media for safeguarding the data and information by

[106] 'Egypt: Draft Law on E-Commerce' (2001) Vol. 16 No. 3 *Arab Law Quarterly* 288-294 retrieved from https://www.jstor.org/stable/3382177?seq=1#page_scan_tab_contents
[107] ibid
[108] Ibid (65)
[109] Law No 88/2003 promulgating the Law of Central Bank of Egypt
[110] Ibid (106) Article 8

the competent authorities according to the conditions and status specified in the Implementing Regulations'[111].

The privacy is preserved by the current provision; however, no mechanism is stipulated with regards to the encryption process as it is left to the Executive Regulation. The challenge, however, lies in the human and physical resources which would be responsible for handling the execution, which the Egyptian government currently lacks in terms of technological equipment, trained personnel and governmental officials with the modern technically equipped mentality.

Another important aspect covered by the proposed law is the consumer protection. As international authorities and bodies propose guidelines to establish national policies for consumer protection such as UNCTAD[112] that encourage good practices with regards to e-commerce tackling areas such as information disclosure, contractual terms, consumer privacy and data security as well as dispute resolution mechanisms, Egyptian draft law followed the said principles by incorporating provisions tackling consumer protection in Articles 15-21 and settlement of disputes in Articles 31 and 32 of the Draft Law.

Consumer protection articles oblige the seller to provide mandatory data as specified in the Executive Regulation (which is yet to be drafted)[113] and oblige parties to electronic transaction to fulfill the contents of the advertisement which are considered 'contractual documents complimentary to the contracts concluded for obtaining advertised commodities and services'[114]. Data protection is granted in Article 17 which stipulates that any personal or bank data of any client obtained by the Authority cannot be kept for a longer than needed time for transaction or used for other than transaction purposes without the written consent of the owner of such data. Furthermore, the seller is prohibited to insert the condition releasing the seller from responsibility associated with financial return and reduction[115] and grants the buyer a right to cancel e-contract within fifteen days from delivery of goods or from the date of contracting for the rendering of the service without any need for further justification[116]. Importantly, the consumer protection article contains a provision which stipulates that: 'any agreement contrary to the contents of this article is considered to be invalid, except the agreements including provisions for protecting the consumer'[117].

[111] Ibid Article 9
[112] 'Consumer Protection in Electronic Commerce' (2017) United Nations Conference on Trade and Development (UNCTAD), TD/B/C.I/CPLP/7 accessed 26 November 2017 at http://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf
[113] Article 15
[114] Article 16
[115] Article 19
[116] Article 20
[117] Ibid (106)

In terms of dispute resolution mechanism, the draft law is less transparent and adaptable for the parties. Article 31 grants powers to the competent Minister and is not very clear with regards to the effectiveness of the mechanism in resolution of both domestic and cross-border e-commerce disputes. It is stated that a special committee is to be formed by virtue of resolution of the competent Minister and is to be chaired by the Vice-President of the State Council and membership of two counselors of the State Council as well as an expert and a high-ranking administration staff all appointed by the Minister[118]. However, neither the timeline nor the cost burdens are being provided for, except for the thirty-day timeframe for appealing the decision of the committee.

Another crucial aspect partially covered by the Draft Law is related to crimes and penalties, and here, it must be said that the Draft Law offers a very poor coverage specifically taking into consideration that cybercrime and crime related to electronic transactions are not provided for in any other existing laws. Although electronic evidence is tackled with in Article 10 and electronic documents are granted the same legal power as customary ones, the crimes and penaltiese' section only deals with misuse of encryption keys[119] and violations related to electronic signature[120].

Elementary challenges, however, on the digital arena such as hacking and fraud, misrepresentation, and access to protected systems are not addressed. Moreover, issues such as jurisdiction which becomes essential in light of trans-border nature of e-transactions is briefly addressed in Article 3 of the Draft E-Commerce Law. Another crucial challenge which is covered partially is the evidence, and in particular loss of it wherein it is destroyed by the perpetrators or camouflaged in a different than electronic crime jurisdiction, and hence, further collection from another location in another country[121] becomes another point of focus which needs to be legally covered.

Furthermore, legislation regulating e-finance which is emerging and going hand-in-hand with e-commerce is another loophole in Egyptian legislation. Online banking, electronic financial operations and mobile payment services are not directly addressed by the Egyptian legislation but are rather scarcely covered by few regulations of the Central Bank of Egypt (CBE) and E-Signature Law. The Decision issued by the Executive Director of the Anti-Money Laundering Unit[122] stipulates a mandatory periodic risk analysis of the system, including penetration tests and ethical hacking. Additionally, it stipulates that 'IT structure which operates online banking must contain firewalls', intruder detection systems, data file and system integrity checking as well as surveillance and incidental response procedures. Also

[118] Article 31
[119] Article 29
[120] Article 30
[121] K M B Islam, 'E-Commerce: Laws and Cybercrime' accessed 25 November 2017 at https://www.academia.edu/694983/E-COMMERCE_LAWS_AND_CYBER_CRIMES
[122] CBE Decision (14 April 2011)

measures in relation to physical security of access to programs, networks, equipment, and protection of encoding keys are stipulated, with the CBE being the responsible authority for supervision and compliance with measures and specifications.

Decision from 2 February 2010 issued by the Board of Directors of the CBE[123] imposes obligation on the bank operating mobile payment services to ensure proper identification of the system's customers and proper authorization for accessing the system.

Elsewise, the electronic payment sector remains very much uncovered by the legislation.

2.1.5 Electronic Contracts and the Challenge

With the rapid growth of e-commerce globally, electronic contracts have become essential element in digital relationships between the parties. Speaking legal language, e-contracts have posed a number of challenges to civil and commercial laws of jurisdictions, namely in relation to time, subject, place of transmission and reception and parties to the contract, and contract rules related to attribution, acknowledgement of receipt, automated and carriage contracts[124]. Current Egyptian legal system does not deal with the above concepts. It does not identify when the e-contract was concluded, whether it was at the time the e-mail was sent accepting the deal, the time of its arrival to the server, or the moment it arrived to the inbox of the receiving party. Leave alone the time element, current legal system does not provide comprehensive definition for the subject of the contract, as current laws deal with goods and services[125] and do not provide guidelines with regards to electronic goods sold online such as electronic computer programs and musical records. In addition, the contract subject related matter becomes even more important when it comes to treatment of transactions for goods which are restricted in Egypt such as cigarettes and alcohol. Without special provisions and definitions stipulated by the current law, the question arises of how electronic transactions involving such goods shall be treated.

Important to note, that even the Draft Law on E-commerce, scarcely covers electronic contracts. In definitions section of the said law, an electronic contract is defined as: 'a contract which expresses the will of one or two parties, or to be negotiated, or to exchange its documents partially or completely through electronic media'[126]. Articles 2, 3 address electronic contracts, Article 2 discusses competent jurisdiction: 'the contractual obligations in the context of the provision of this Law are governed by the law of the state where the common domicile of the two contracting parties is, if both are of different domiciles then the law of the state where the contract was concluded

[123] CBE Decision (2 February 2010)
[124] Ibid (67)
[125] S Mason, *Electronic Signature in Law* (Cambridge University Press, 2012)
[126] Ibid (106)

will govern, unless the two contracting parties have agreed otherwise; the contract will be considered as concluded as soon as receipt is acknowledged'[127]. Article 3 states that: 'from a formal point of view the electronic contracts will be governed by the same Law that governs its substantive provisions'[128]. Crucial to notice, that the only two articles dealing with the contracts do not refer to Executive Regulations of the law, which normally would provide detailed guidance on execution of the law.

As of today, the E-Signature Law No. 15 of 2004 remains the first and the only legislative response to electronic transactions in Egypt, which enables the use of electronic means to 'issue, exchange, and store documents, thereby guaranteeing the credibility and enforceability of electronic transactions, and preserving the rights of those undertaking them'[129]. The scope of the law covers civil, commercial, as well as governmental transactions. The Law permits to undertake commercial transactions such as sales of goods agreements, export and import agreements, booking of tickets and hotels as well as various banking transactions though the usage of signed electronically documents[130]. However, the overemphasis on encrypted signatures, the Law has 'eliminated the very concept of e-signature before it has had a chance to be used'[131] as the electronic signature 'should not be limited to a numerical signature accompanied by a verification certificate accessible to those licensed to read it'[132] but rather should entail the full spectrum of signatures including but not limited to signatures at the end of the body of a mail, handwritten signatures scanned and inserted into the electronic text. Companies as well as consumers would not be as much interested in numerical encrypted signatures as much as they would be in utilization of wide-spectrum e-signatures together with detailed provisions covering electronic commerce transactions and their consequences, noting specifically that companies already have certain systems in place for secure exchange of information such as SWIFT system used between different banks[133].

Speaking of loopholes in the Egyptian legislation and coming back to the matter of jurisdiction as one of the crucial aspects of the international e-commerce, as noted by Blythe[134] in his article, Egypt should formally 'state its claim to a long-arm jurisdiction against any party who is a resident or citizen of a foreign country, so long as that party has established minimum contracts with Egypt'[135], whereby a minimum contract will exist if an e-seller outside of Egypt sells goods or services to a party residing within Egypt. And hence, the E-Commerce Law should not allow for evasion

[127] Ibid Article 2
[128] Ibid Article 3
[129] F Amereller, K Balz, S Klaiber, 'A Guide to Business Law in Egypt' (2010) accessed 10 December 2017 at http://amereller.com/wp-content/uploads/2016/10/Amereller_Egypt-Guide-2010.pdf
[130] Ibid 207
[131] Ibid (80)
[132] ibid
[133] ibid
[134] Ibid (67)
[135] ibid

of the Egyptian courts' jurisdiction for the parties not physically present in Egyptian territory.

3. Lessons Learned from the E-Commerce Legislation of the South Africa and the United Kingdom

3.1 E-Commerce Legislation of South Africa

3.1.1 Overview

Electronic Communications and Transactions Act 2002[136] of South Africa, enforced in 2002 provides a legal framework for electronic transactions, and 'principally afforded electronic communications and transactions legal force and effect'[137]. South Africa's e-commerce law, the ECTA, following the principles of UNCITRAL Model Law, provides an enabling legal framework by dealing with and offering guidance on e-contracts, online consumer protection, cryptography, cybercrime, protection of privacy, and production of electronic evidence in courts[138].

3.1.2 E-signatures

The ECTA recognized electronic signatures as 'a facility for legal assurance in electronic commerce'[139] by treating e-signatures as a functional equivalent of handwritten signatures for the purpose of electronic transactions. The ECTA identifies two types of e-signatures: a) an 'electronic signature' defined as 'data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'[140]; and b) 'advanced electronic signature', 'AeS', defined as 'an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37'[141].

AeS is required in instances when 'the signature of a person is required by law and such law does not specify the type of signature'[142] for the purposes of concluding a certain electronic transaction. The Act provides that AeS is to be used in instances where 'statement or document is to be notarized, acknowledged, verified or made under oath'[143]

[136] Electronic Communications and Transactions Act 25 of 2002 (ECTA)
[137] P Chetty, 'An Analysis of Electronic Signature Regulation in South Africa' (2013) *A research report submitted to the Faculty of Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management (in the field of ICT Policy and Regulation).*
[138] Ibid; Z N Jobodwana, 'E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges' (2009) *Journal of International Law and Technology,* Vol. 4 Issue 4
[139] R Low, S Christensen, 'E-signatures and PKI Frameworks in Australia.' (2004) *The Digital Evidence Journal, incorporating the e-Signature Law Journal* 1(2): pp. 56-59.
[140] ECTA, Chapter 1, Section 1
[141] ibid
[142] Ibid, Section 13
[143] Ibid, Section 18, 19

Meanwhile, the parties may agree to the form of acceptable e-signature. The main objective of the AeS and its accreditation is to ensure higher security of e-transactions[144], and hence, the criteria for accreditation of the AeS include and must demonstrate the following: that e-signature 'a) is uniquely linked to the user; b) is capable of identifying this user; c) is created using means that can be maintained under the sole control of that user; and; d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable; e) is based on the face-to-face identification of the user.'[145] Further powers and authorities in relation to accreditation is granted to the Minister in Section 41 of the Act.

The ECTA, in Section 13(5), further provides for an expression of intent for instances when the e-signature is not required[146].

Evidential weight and requirements for legal validity are addressed in Sections 13, 14 and 15 of the Act. Sections 14 and 15, cover the assessment of originality and evidential weight[147]. The integrity is assessed: 'a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display; b) in the light of the purpose for which the information was generated; and c) having regard to all other relevant circumstances'[148]; whereas the evidential weight is addressed in Section 15(3), and is assessed taking into consideration the following factors: 'a) the reliability of the manner in which the data message was generated, stored or communicated; b) the reliability of the manner in which the integrity of the data message was maintained; c) the manner in which its originator was identified; and (d) any other relevant factor.'[149]

Legal validity requirements are provided for in Section 13 of the Act and differ for e-signatures as opposed to AeS. With regards to the e-signature as defined in Section 1, for it to be considered acceptable it should demonstrate a 'method used to identify the person and to indicate the person's approval of the information communicated' and a regard given to 'all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated'[150]. As for the advanced electronic signature, which is accredited is to be considered to have been applied appropriately unless proven

[144] Ibid (137)
[145] Ibid (136), Section 38
[146] Ibid Section 13(5): 'Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that- (a) it is in the form of a data message; or (b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred'.
[147] Ibid (137)
[148] Ibid (136), Section 14(2)
[149] Ibid, Section 15(3)
[150] Ibid (136) Section 13

to the contrary.[151]Therefore, a user of an AeS enjoys the 'added benefit of placing the onus of disproving its legal validity on the contesting party'[152].

3.1.3 Regulation of Foreign E-signature Products and Services

Foreign authentication products and services, or foreign providers may be granted recognition of accreditation or granted recognition by the competent Minister, as per Section 40 of the Act. Forming a false perception of accreditation by foreign providers is deemed an offence[153].

3.1.4 E-Signatures in E-Government Services

South Africa is one of the countries[154] legislation and regulations of which recognize e-government. ETCA allows electronic filing, recognizes e-signatures and e-evidence. E-government services including issuing permits, licenses and approvals, e-payment of governmental fees are covered in Sections 27 and 28 of the Act. Requirements for filing are further specified in Section 28 of the ECTA, whereby it is the competent public entity which is granted the authority to specify the requirements of form of signature and its format, 'the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message'[155] by means of publication of such requirements in the governmental official Gazette[156]. The Act also identifies South African Post Office Limited (SAPO) as the preferred authentication service provider for the purpose of Section 28 of the Act.

3.1.5 The Accreditation Authority

Similar to the Egypt's ITIDA, the ECTA of South Africa in Chapter 6 addresses the Accreditation Authority, its appointment and powers, the process and criteria of accreditation, termination and revocation of accreditation. The Act grants further powers to the Minister to issue additional regulations in these regards[157]. The Accreditation Authority as referred to in the ECTA is empowered to monitor the conduct, systems and operations of the authentication service provider as well is empowered to suspend, revoke accreditation an appoint auditing firms for the purpose of assessment of compliance with the criteria of accreditation as set forth in the Act. Further, the Authority is obliged to maintain a database accessible by the public which contains information about accreditations, revoked accreditations, recognitions granted to foreign providers[158] which is meant to enable transparency with the public.

---

[151] ibid
[152] Ibid (137)
[153] Ibid (136), Section 40(2)
[154] Among Australia, Malaysia, Singapore, Canada; A J Mambi, *ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community* (African Books Collective, 2010) 172
[155] Ibid (136) S 28
[156] Ibid Section 28
[157] Ibid, Section 41
[158] Ibid, Section 36

3.1.6 International Electronic Transactions and Jurisdiction

The ECTA provides for international agreements unlike the legislation of Egypt, whereby it states in Section 47 that 'the protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the agreement in question'[159]. And, hence, the ECTA predicts the conclusion of agreements that involve parties from different jurisdictions and further provides for applicability of consumer protection provisions as set forth in Chapter 7 of the Act to international agreements irrespective of the legal system applicable to a given agreement[160].

The ECTA in Section 90 deals with the jurisdiction and provides for instances where courts of South Africa will have jurisdiction[161] over disputes arising out of electronic contracts as well as outlines protective measures available. The Act in principle protects a South African consumer entering into an e-contract which is authorized by the ECTA and such protection is availed to the consumer irrespective of the governing law of the contract and in the event of absence of the choice of law clause[162].

Important aspect of the legislation related to the principles of conflict of laws, is contained in Section 22 of the Act which states that the place of the contract 'is the place where the acceptance of the offer is received'[163]. Further, Section 23(c) states that message 'must be regarded as having been received at the addressee'**s** usual place of business or residence'[164]. However, given the fact that e-mail can be accessed anywhere in the world, and hosting of the mail might be located in a different place than the location or residence of the offeror, the provisions of the ECTA do not cover the aspect.

3.1.7 Electronic Contract

Section 22(1) of the Act addresses the formation and validity of e-contracts: 'an agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages'[165]. The ECTA contains provisions to enable electronic contracts and legally binding e-signatures. Wrap agreements can be deemed covered by virtue of provisions under Section 13(5) which stipulates that 'any other expression of intent or statement is not without legal force and effect merely on the grounds that; (a) it is in the form of a data message; or (b) it is not evidenced by an

[159] Ibid Section 47

[160] C Erasmus, 'Consumer Protection in International Electronic Contracts' (2011) Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Magister Legum* in Import and Export Law at the Potchefstroom campus of the North-West University.

[161] Ibid (ECTA), Section 90: (a) the offence was committed in the Republic; *(b)* any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic; *(c)* the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or *(d)* the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

[162] Ibid (137)

[163] Ibid (138) 292

[164] Ibid (136)

[165] Ibid Section 22(1)

electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred'[166].

According to the Act, a data message shall be considered received by the addressee 'when the complete message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee'[167]. And, therefore, an agreement will be deemed as concluded at the moment when the data message containing the acceptance enters the information system of the offeror and is capable of being retrieved by the offeror[168]. The general rule is that the acceptance must be received by the offeror[169]. Under ECTA, as soon as acceptance enters the information system of the offeror, the offer cannot be withdrawn[170].

Section 46 of the ECTA deals with the performance of the e-contracts, which obliges the supplier to execute the order within 30 days from the day of receipt of the order unless there is an agreement between the parties to the contrary. In case of failure of the supplier to fulfill the order within the prescribed period, the consumer is entitled to the right to cancel the contract within 7 days' written notice. Furthermore, in case of unavailability of the offered goods and/or services, the consumer is entitled to receive refund of payments within 30 days period from the date of notification by supplier[171].

3.1.8 Consumer Protection

The ECTA addresses consumer protection in very specific terms, and hence, grants benefit to consumers and presents an obstacle to the online traders in a sense that anyone conducting business online would have to be acquainted with the regulations in order to tailor their online business activities accordingly. The provisions under the Act, however, are applicable to consumer transaction and not business-to-business[172].

A consumer under the Act is defined as 'any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier'[173], and hence, as mentioned above the scope of protection is limited to natural persons.

Section 48 of the ECTA prevents parties from concluding agreements avoiding application of the Act's provisions, and hence, as prescribed by the ECTA any 'provision in an agreement which excludes any rights provided for in this Chapter is null and void'[174].

[166] Ibid Section 13(5)
[167] Ibid Section 23(b)
[168] Ibid (138)
[169] R H Christie, *The Law of Contract in South Africa* (LexisNexis/Butterworths, 2006)
[170] ECTA Section 23(b); ibid (138)
[171] ECTA, Section 46 (1-3)
[172] ibid (55) 54
[173] ECTA, Section 1
[174] ECTA, Section 48

Section 43(1) of the Act obliges suppliers trading online to avail certain information to consumers on the website where the goods and services are offered, including but not limited to supplier's full name and legal status, physical address, contact details of the company, method of payment, return and refund policy, code of conduct.

Further, Section 43(2) offers another safeguard to a consumer and places an additional burden on the supplier whereby, the supplier is being placed under the responsibility to avail an opportunity to the consumer to review an electronic transaction prior to its conclusion, and correct mistakes, if any, or withdraw from the transaction. In case of failure of a supplier to provide the consumer with such an opportunity, the consumer is granted the right to cancel the transaction within '14 days of receiving the goods or services under the transaction'[175]. And therefore, Section 43 ensures that the consumer possesses sufficient information in order to make an informative choice pertinent to the electronic transaction he is concluding.

Further protection to consumer is available under Section 44 of the Act, which entitles a consumer to a 'cooling-off period' whereby a consumer has the right to cancel 'without reason and without penalty any transaction and any related credit agreement for the supply'[176] within 7 days from the date of receipt of goods or after 7 days from the date of conclusion of the agreement for the services[177].

Important to note, that certain transactions are excluded from the scope of the Act, and notably, financial services, insurance and reinsurance transactions, dealings in securities and banking transactions, auctions, supply of goods for daily consumption and food, as well as goods and services which are dependant on 'fluctuations in the financial markets and which cannot be controlled by the supplier'[178].

3.1.9 Cybercrime

Last but not least, Chapter 13 of the ECTA seeks to make the first statutory provisions on cybercrime in South African jurisprudence. The Act seeks to introduce statutory criminal offences relating to the following:

- unauthorized access to data (e.g. so-called "hacking" and trading in passwords used to commit an offence);
- interception with data (e.g. tapping into data flows or denial of service attacks);
- interference with data (e.g. viruses and denial of service attacks);
- computer related extortion, fraud and forgery (e.g. where someone gains financially by undertaking to cease or desist from doing something using a computer).

[175] ECTA, S 43(2)
[176] ECTA Section 44
[177] ECTA; W Jacobs, PN Stoop, R Van Niekerk, 'Fundamental Consumer Rights under the Consumer Protection Act 2002: A Critical Overview and Analysis' (2010) *Potchefstroom Elec LJ* 303.
[178] Ibid (138)

Any person aiding or abetting another in the performance of any of these crimes will be guilty as an accessory. The ECTA prescribes the penalties for those convicted of offences which render a person liable to a fine or imprisonment for periods not exceeding 12 months in certain circumstances or five years in certain circumstances.

3.2 Comparison of Legislation (Egypt and South Africa) and Lessons Learned from South Africa's ECTA

This section aims to compare e-commerce laws of Egypt (E-Signature Law No.15/2004, Draft Law on E-Commerce) and the ECTA 2002 of South Africa, covered in preceding section in order to identify major differences and certain aspects of the ECTA which might be beneficial to Egyptian legislators as they are progressing with their efforts on the arena of e-commerce related legislation.

3.2.1 E-Signatures

One significant and major difference between the two legislative instruments discussed herein lies in definition of e-signature and its applicability to electronic transactions. Whereas ECTA identifies two types, 'an electronic signature' and 'an advanced electronic signature', its Egyptian counterpart[179]provides one definition: 'E-signature: What is on an electronically written message in the form of letters, digits, codes, signals or others and has a unique identity that identifies the signer and uniquely distinguishes him/her from others'[180]. And although, the definition seems to combine both e-signature and AeS equivalents of the ECTA, the definition corresponds to AeS only, as the Egyptian Law and its Executive Regulation[181] deals with encrypted signature supported by certificate. And therefore, Section 13 of ECTA which deals with instances of usage of the two types of signatures as defined by the Act, in its Egyptian counterpart becomes irrelevant and is substituted by Article 14 which states: 'Within the scope of civil, commercial and administrative transactions, e-signatures shall have the same determinative effect that signatures have under the provisions of the Evidence Law in the civil and commercial articles, if the creation and completion thereof come in compliance with the terms stipulated in this Law and the technical and technological rules identified in the Executive Regulations of this law'[182]. Evidential weight and legal validity (as addressed in Sections 13-15 of the ECTA) are similarly covered by the Egyptian legislation in Articles 17, 18[183] and Articles 2, 3 and 4 of its Executive Regulation which provide criteria for formation of the e-signature secured creation data.

The Lesson Learned

[179] Law No. 15 of the year 2004
[180] Ibid Article 1(c)
[181] Decree No. 109 of the year 2005
[182] Ibid (178)
[183] Article 17: 'Unless stipulated in this Law or the Executive Regulations thereof, the provisions of the Evidence Law in the civil and commercial articles shall prevail in relation to proving the validity of the official and unofficial electronically written messages, e-signatures and e-writings'; Article 18: 'The e-signatures, e-writing, and electronically written messages shall have the determinative effect for evidence provided their compliance with the following: A. The e-signature is for the signer solely B. The signer has sole control over the electronic medium C. Possible discovery of any modification or replacement of the data of electronically written message or e-signature. The Executive Regulations of this Law shall set out the necessary technical and technological rules'.

The South African ECTA comprises a very significant advantage over Egypt's E-Signature Law No. 15/2004, which is inclusion of a non-encrypted electronic signature. Egypt's law by focusing on encrypted signatures, has abandoned the concept of e-signature as related to its application in the context of e-commerce and electronic transactions as an e-signature for such purposes should not be 'limited to a numerical signature accompanied by a verification certificate accessible to those licensed to read it'[184] but rather shall encompass a full range of digital signatures such as signatures at the end of e-mail, signatures interpolated into an electronic message, any signature which can be identified and can be verifiable, for example. The reason for arguing for such an inclusion is practicality in application when it comes to e-commerce, as companies and individual consumers are unlikely to favor encrypted signatures. As for the companies, operating in the digital era, they already utilize systems to exchange information such as for example, SWIFT system used by the banks and Intranet systems by other companies, and hence, it is unclear what will be the benefit for the companies or what would be the trigger, not to mention individual consumers, to purchase verification certificates, process of obtainment of which is not very simple and which need to be renewed on regular basis[185].

3.2.2 Regulation of Foreign E-Signature Products

Similar to Section 40 of the ECTA, Egypt's regulation, allows accreditation of foreign entities concerned with issuing the digital certificates, as per provisions in Article 22 of the E-Signature Law and Articles 21, 22 of its Executive Regulation. As opposed to the South African legislation, it is more detailed[186].

3.2.3 E-Signature and E-Government Services

E-government services is clearly one of the areas that is not directly addressed and dealt with by the Egyptian legislation as opposed to ECTA of South Africa, which provides for government services in Sections 27 and 28. In general, in Egypt, the lack of comprehensive legal framework for e-government has slowed the implementation of e-government services such as tax filing, online payment of governmental fees, issuing title documents and other certificates[187]. Implementation of the e-government services remains 'restricted without a legal equivalence between digital and paper processes'[188]. Although design and deployment of e-signatures are covered by E-Signature Law of 2004, however, it seems that 'no PKI-provider on the Egyptian market was able to fulfill the ambitious specific requirements established until 2010[189]. Moreover, according to the OECD studies[190] governmental officials of Egypt are lacking awareness of the 'status and

[184] Ibid (80)
[185] Ibid (80)
[186] Decree No. 109/2005, see Article 21
[187] T R Gebba, M R Zakaria, 'E-Government in Egypt: An Analysis of Practices and Challenges' (2015) *International Journal of Business Research and Development* Vol. 4 Issue 2, pp 11-25
[188] ibid
[189] 'OECD E-Government Studies: Egypt 2013' (OECD Publishing, 2013), p. 70
[190] ibid

extent of the current legislation and its possibilities'[191], further governmental officials were referring to the 'complexity of regulations and to the difficulty of understanding laws or decrees'[192]. Noteworthy, that neither E-Signature Law No. 15/2004 nor its Executive Regulation addresses directly e-government services and application of e-signature and e-writings in this regard.

The Lesson Learned

To avoid ambiguity and instill clarity of Egypt's regulations, the Egyptian legislators should have considered or shall consider inclusion of provisions similar to Sections 27 and 28 of the South Africa's ETCA with regards to acceptance of authenticated documents, electronic filings, recognition of e-signatures and specification of their types by different governmental entities for the purpose of providing e-government services to the public.

3.2.4 Jurisdiction

A matter of jurisdiction, as previously noted shall be incorporated into Egypt's E-Commerce legislation. A good example, is the South Africa's ECTA which avails protection to South African consumers by granting jurisdiction to South African courts over disputes arising out of e-contracts and availing protective measures. And, therefore, the ECTA might be a good source of information for Egyptian legislators with these regards.

3.2.6 E-Contracts

Comparing Egypt's Draft Law on E-Commerce and relevant provisions of the ECTA, it becomes obvious that provisions of the Egyptian legislation are too broad and limited. In particular, Egyptian legislators may benefit from Sections 22(2) and 46 of the ECTA when considering Draft Law on E-Commerce for ratification.

3.2.7 Consumer Protection

In terms of provisions related to consumer protection, the ECTA of South Africa and Draft Law on E-Commerce of Egypt, mirror each other. Article 15 of Egypt's draft law mirrors its counterpart Section 43(1) which obliges suppliers trading online to provide certain information to the consumer. Article 19 deals with refund and obligations of the supplier similar to Section 43 of the ECTA. Article 20, similar to Section 43(2) provides for the right to the consumer to cancel the transaction within 15 days as opposed to 14 days granted under ETCA. Article 21 reflects Section 48 of the ECTA, which prevents parties from concluding agreements outside the scope of application of the Law's provisions[193].

[191] ibid
[192] ibid
[193] Egypt's Draft Law on E-Commerce, Article 21: 'Any agreement contrary to the contents of this article is considered to be invalid, except the agreements including provisions for protecting the consumer'.

Therefore, regulations of both countries with regards to consumer protection seem to be very much similar, with Egypt having incorporated standard provisions enabling protection of its consumers.

3.2.8 Cybercrime

Cybercrime is one of the sections available under the ECTA which might be taken into consideration by Egyptian legislators, as currently, the scope of crimes and penalties under the Egyptian E-Signature Law and Draft Law on E-Commerce as provided for in Article 23 of the E-Signature Law and Articles 29, 30 of the Draft Law on E-commerce, respectively, is limited to: a) issuing digital certificates without obtaining a license from the Authority to practice this activity; b) Destroying or damaging a signature, electronic medium or electronically written messages; or falsifying any of these by imitation, modification, alteration or by any other means; c) Using knowingly a falsified or damaged signature, electronic medium or electronically written messages; d) Managing through any means to obtain unrightfully a signature, written message or electronic medium; or breaching, intercepting or putting such electronic media out of service[194]. The scope of crimes and penalties as provided for under the ECTA is still in the stage of legislation procedures which shall be reflected in the Cybercrime Law of Egypt, which is yet in the draft form[195].

3.3 E-Commerce Legislation of the UK

3.3.1 Introduction

English law governing e-commerce is set out in an ample of different statutory instruments, both, specific to the conduct of online business activities and, general, applicable to all business transactions. The e-commerce related regulations and law provisions are rooted in the EU laws[196] and, hence, are subject to increasing harmonization at the EU level, although it is unclear whether EU regulations will continue to further impact UK legal framework following the decision of the UK to exit EU.

The below selected regulations represent particular significance in terms of e-commerce, however, not all of them will be addressed in the process of comparison of legislation instruments for the purpose of this dissertation and its scope.

- *The Electronic Commerce (EC Directive) Regulations 2002*[197] which imposes obligations on the service provider, in particular related to provision of certain information to the consumer, quality and content of the service provided but not the requirements applicable to goods as such or to their delivery;

[194] E-Signature Law No. 15/2004

[195] H El-Mahdaw, 'Is the Government Watching Egyptians or Watching Over Them: Egypt's Cyber Crime Law in January' (Tuesday, 3 January, 2017) Ahram Online accessed 18 February 2018 at http://english.ahram.org.eg/NewsContent/1/64/253973/Egypt/Politics-/Is-the-government-watching-Egyptians-or-watching-o.aspx

[196] Ibid (160)

[197] The Electronic Commerce (EC Directive) Regulations 2002 No. 2013

- *The Consumer Rights Act 2015*[198] *(CRA)* consolidates a range of earlier UK consumer rights legislation, provides updated section on the remedies for breach available to the consumer, covers consumer contracts for goods, digital content and services;

- *The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013*[199] *(Consumer Contract Regulations)* introduces additional obligations on online traders of goods and services who deal with consumers[200];

- *The Data Protection Act 1998*[201] *(DPA)* regulates processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information;

- *The Privacy and Electronic Communications (EC Directive) Regulations 2003*[202] *(PEC Regulations)* provides guidance related to solicited and unsolicited marketing activities via e-communication;

- Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (2016 No.696)[203] (the 'eIDAS') deals with electronic identification systems and establishes a legal framework which enables recognition of such systems between Member States, addresses Trust Services, introduces a legal framework for e-signatures, e-seals, time stamps, website authentication[204]. The eIDAS regulation has revoked the Electronic Signatures Regulations 2002;

- Consumer Protection (Distance Selling) Regulations 2000 No. 2334[205] is dealing with consumer protection and is not applicable to transactions of a "business to business" nature;

- Electronic Communication Act 2000[206] and the Electronic Signatures Regulations 2002[207]

This section aims to analyze the UK legal framework for electronic commerce in comparative angle related to the matters discussed and covered by the legislation of

[198] Consumer Rights Act 2015
[199] The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 No. 3134
[200] The Consumer Protection (Distance Selling) Regulations 2000 No. 2334 do not apply to contracts entered on or after 13th of June 2014
[201] The Data Protection Act 1998
[202] The Privacy and Electronic Communications (EC Directive) Regulations 2003 No. 2426
[203] Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (2016 No.696) (The Regulation (EU) No 910/2014 (the 'eIDAS Regulation') repealed and replaced the e-Signatures Directive (1999/93/EC) and is directly applicable in the 28 Member States of the European Union.
[204] 'Electronic Signatures and Trust Services Guide' Department for Business, Energy, and Industrial Strategy accessed 20 February 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf
[205] Ibid (200)
[206] Electronic Communication Act 2000
[207] Electronic Signatures Regulations 2002 No. 318

Egypt and South Africa, and in particular UK's legal provisions related to e-contracts, e-signatures, e-government, jurisdictional matters, consumer protection and cybercrime.

3.3.2 E-signatures

Under English law, for a contract to be deemed valid, a written signature is not a necessary requirement, as a contract is generally valid if parties with legal competence have reached an agreement, whether verbally, electronically or by means of a physical paper document. Case law confirms the postulate above, as is evidenced in the decision of the Court of Appeal in the case of *Golden Ocean Group v Salgaocar Mining Industries*[208] which confirmed that contracts cannot be denied enforceability merely because they are concluded electronically, and that e-mails which constituted a contract were signed by the electronically printed signature of the senders.

UK has implemented the EU Directive 1999/93[209] on Electronic Signatures by enforcing its Electronic Communication Act 2000 which recognized e-signatures, and addressed encryption and certification schemes, and attempted to facilitate e-commerce by removing requirements to non-electronic writing and signatures[210]. Further, the Electronic Communication Act was followed by the Electronic Signatures Regulations in 2002 which introduced further guidance with regards to supervision and liability of certification services providers and matters related to data protection[211].

Further development of the legislative landscape in this area happened in 2016 whereby EU E-Signatures Directive 1999/93/EC[212] has been repealed and replaced by Regulation (EU) No. 910/2014[213] (the "*eIDAS Regulation*") which came into force on 1 July 2016 and was subsequently adopted in the UK by virtue of Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (2016 No.696)[214].

Previously, the UK legislation had adopted a two-tier system of e-signatures which recognized the advanced electronic signatures and basic electronic signature as per Electronic Signatures Regulation Act 2002[215], however, the new *eIDAS Regulation*[216] has revoked the Electronic Signatures Regulation Act 2002. And, hence, now a three-tier

---

[208] *Golden Ocean Group v Salgaocar Mining Industries* [2011] EWHC 56 (Comm)

[209] Directive 1999/93 of the European Parliament and Council on a Community Framework for Electronic Signatures

[210] I J Lloyd, *Information Technology Law* (6th edn, Oxford University Press 2011)

[211] A A Alajaji, 'An Evaluation of E-Commerce Legislation in GCC States: Lessons and Principles from the International Best Practices (EU, UK, UNCITRAL)' (2016) Submitted for the degree of Doctor of Philosophy

[212] Ibid (EC 1999/93)

[213] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the *"eIDAS Regulation"*)

[214] Ibid (203)

[215] '"advanced electronic signature" means an electronic signature— (a) which is uniquely linked to the signatory, (b) which is capable of identifying the signatory, (c) which is created using means that the signatory can maintain under his sole control, and (d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable'[215]; and

'"electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'

[216] Ibid (203)

system is adopted as provided for in the EU Regulation (910/2014), which identifies three types of electronic signatures:

'Electronic signature' (SES) means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign[217];

'Advanced electronic signature' (AES) means an electronic signature which meets the requirements set out in Article 26[218];

'Qualified electronic signature' (QES) means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures[219];

Qualified E-Signatures are Advanced E-Signatures created by a qualified e-signature creation device, based on Qualified Certificates, which can be only be used by a qualified trust service provider by the Supervisory Body. The creation data must be stored on a device such as USB token or a smart card[220].

Acceptance of the lower tier signatures (non-advanced) is provided for in Section 7 of the Electronic Communication Act[221] as amended by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016[222]:

'(1) In any legal proceedings— a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data. (2) For the purposes of this section an electronic signature is so much of anything in electronic form as— (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and (b) purports to be used by the individual creating it to sign.'[223]

Further, the amended legal instrument introduced additions to Section 7 of the Communication Act 2000, and recognized electronic seals and related certificates, electronic time stamps and related certificates, electronic documents and related certificates, electronic registered delivery service and related certificates[224].

It is important to note, that one of the major changes introduced by the UK's eIDAS Regulation is that e-signatures can now be used by individuals only, whereas eIDAS

[217] Ibid (EU eIDAS 910/2014) Article 3(10)
[218] Ibid Article 3(11)
[219] Ibid Article 3(12)
[220] Ibid (204)
[221] Ibid (206)
[222] Ibid (203) Schedule 3
[223] ibid
[224] Ibid (203) Schedule 3(1)

differentiates between natural and legal persons, and, hence, introduces legal seals for the sole usage by legal persons, i.e. corporate entities.

Taking into consideration definitions available under the two Acts and Section 7 of the Communications Act, it can be deducted that UK law recognizes most forms of the e-signatures. Although UK legislation does not directly address the matter of e-mail address, typed name interpolated into an electronic message, it seems that common law takes a flexible stance with regards to acceptance of new forms of signatures[225].

However, it is important to point out that although UK legal framework is quite detailed with regards to e-signatures and common law approach being flexible, yet, some difficulties are faced when it comes to the current dealings in the realm of e-transactions as is evident in the recent judgment in *Mehta v J Pereira Fernandes SA*[226] where it was ruled that automatic insertion of an e-mail address without name or initials of the sender did not satisfy the requirements and does not constitute a sufficient signature.

The Lesson Learned

UK legislation with regards to e-signatures is similar to the South African ECTA provisions but is definitely more detailed and extensive. It is clearly a good reference for Egyptian legislators, in specific, what concerns the lower tier e-signatures and their recognition, as well as other facilities offered such as electronic seals, time stamps and other provisions of Section 7 as amended by eIDAS Regulation. It might be a good step towards elimination of ambiguity in the Egyptian legal framework to consider definitions and provisions of UK's Electronic Communication Act 2000 and eIDAS Regulation and its implementation.

3.3.3 E-Signature and E-Government Services

UK's eIDAS Regulation facilitates and enables further developments on the arena of e-government services. As online identification is becoming important as services migrate to the online realm, the UK government introduced several platforms including GOV.UK Verify which now enables businesses and natural persons to verify their identity and access governmental services such as filing tax reports, checking and updating company car tax, among a range of other services available for use on the platform. eIDAS further enables the government to work on introduction of other services such as digital mortgage service, for example[227].

3.3.4 E-Contracts

Electronic Commerce (EC) Directive Regulations 2002[228] defines 'commercial communication' as 'a communication, in any form, designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial

[225] *Jenkins v Gaisford* [1863] 3 Sw & T 93; *Bennet v Brumfitt* [1867-1868] LR 3 CP 28; *Newborne v Sensolid* [1954] 1 QB 45; *Godwin v Francis* [1870] LR 5 CP 295

[226] *Mehta v J Pereira Fernandes SA* [2006] EWHC 813

[227] 'Executing a Document Using Electronic Signature' (2017) HM Registry accessed 20 February 2018 at https://hmlandregistry.blog.gov.uk/2017/02/08/executing-document-electronic-signature/

[228] Ibid (197)

or craft activity…'[229]. The definition is broad enough to incorporate electronic contracts concluded by e-mail, electronic data interchange and web-based transactions. Regulation 7 of the Directive obliges service providers to 'clearly identify' promotional offers and to 'ensure that any conditions which must be met to qualify for it are easily accessible and presented clearly and unambiguously'[230]. Notably, the Regulation does not provide further guidance in terms of what constitutes a 'clearly identifiable' manner neither does it define a 'promotional offer'. Noteworthy, the regulation deals with promotional offers and does not directly address invitation to treat in consideration of the technical features of automated websites.

Under English contract law, significant importance is availed to the recognition of offer and acceptance for the purpose of building legal effects. Substantive rules on the placing of the order are contained in Regulation 11[231] of the Electronic Commerce (EC Directive) Regulations 2002[232] whereby the service provider is obliged to acknowledge receipt of the order 'without undue delay and by electronic means'[233]. An order is defined in Regulation 12 of the Electronic Commerce Regulations 2002, as 'except in relation to regulation 9(1)(c) and regulation 11(1)(b) where "order" shall be the contractual offer, "order" may be but need not be the contractual offer for the purposes of regulations 9 and 11'[234]. However, ambiguity of the wording of the Directive suggests that discretion has been granted to the courts and common law[235]. Similar to the South Africa's ECTA but less precise, the UK counterpart provides that 'the order and the acknowledgement of receipt will be deemed to be received when the parties to whom they are addressed are able to access them'[236]. As is evident, the UK regulation does not deal with contract formation which remains subject to common law and application of the English contract law doctrine, which differentiates between an offer and an invitation to treat. And hence, the court would have to apply a set of rules in order to assess the intention of the parties to enter into a binding contract.

Regulation 9 of the Directive addresses informational and technical requirements imposed on the service provider in conclusion of a contract. And, again, the invitation to treat which has broader implications is not addressed and is left to the discretion of the

[229] Ibid Regulation 2
[230] Ibid Regulation 7(c)
[231] Regulation 11: (1) Unless parties who are not consumers have agreed otherwise, where the recipient of the service places his order through technological means, a service provider shall– (a) acknowledge receipt of the order to the recipient of the service without undue delay and by electronic means; and (b) make available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors prior to the placing of the order. (2) For the purposes of paragraph (1)(a) above— (a) the order and the acknowledgement of receipt will be deemed to be received when the parties to whom they are addressed are able to access them; and (b) the acknowledgement of receipt may take the form of the provision of the service paid for where that service is an information society service. (3) The requirements of paragraph (1) above shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.
[232] Ibid (197)
[233] ibid
[234] ibid
[235] Ibid (211)
[236] Ibid (197) Regulation 11(2)(a)

courts in application of common law principles[237] as illustrated in landmark cases[238]. Therefore, the Regulation provides provisional and partial coverage of the matter by specifying technical steps to be taken by the service provider. Consider Regulation 9(3) which requires the service providers to avail the terms and conditions of the contract in a 'way that allows him to store and reproduce them'[239], however, no further guidance is offered in terms of the form or the way they must be offered, and hence, a degree of ambiguity is present when it comes to dealing with advertisements placed through automated websites which can be easily and frequently updated.

The requirement of making terms available as provided for in the E-Commerce Regulations 2002 is further strengthened, however, in the Consumer Contracts Regulations 2013[240] which emphasizes the 'reasonable expectation principle'[241] in Section 8 which states that: 'something is made available to a consumer only if the consumer can reasonably be expected to know how to access it'[242]. It further provides in Section 5 a 'systematic and constructive explanation'[243] of a 'durable medium' which is defined as:

'paper or email, or any other medium that (a) allows information to be addressed personally to the recipient; (b) enables the recipient to store the information in a way accessible for future reference for a period that is long enough for the purposes of the information; and (c) allows the unchanged reproduction of the information stored.'[244]

According to Wang[245] the definition is 'well-blended' and considers current practices in other jurisdictions as well as facilitates a 'harmonized standard'[246].

3.3.5 Consumer Protection

UK consumer is protected by virtue of several legal instruments and in particular, Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013[247], *The Consumer Rights Act 2015*[248] *and* Consumer Protection (Distance Selling) Regulations 2000[249] among others, which avail protective remedies aiming to protect consumers from uncertainty in relation to the electronic contract and instill confidence with regards to available rights.

---

[237] F Tasneem, 'Enforceability of Electronic Contracts in Australia' (2015) RMT University
[238] *Spencer v Harding* (1870) LR 5 CP 561; *Partridge v Crittenden* (1968) 2 All ER 421; *Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd* (1953) 1 QB 401; *Grainger & Sons v Gough* (1896) AC 325, 334
[239] Ibid (197)
[240] Ibid (199)
[241] F F Wang, 'The Incorporation of Terms into Commercial Contracts: A Reassessment in the Digital Age' (2015) *Journal of Business Law*
[242] Ibid (199) S.8
[243] Ibid (241)
[244] Ibid (199)
[245] Ibid (241)
[246] ibid
[247] Ibid Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013
[248] Ibid (198)
[249] Ibid (205)

One of the significant elements of the Electronic Commerce (EC Directive) Regulations 2002 is that it obliges the service provider to acknowledge the receipt of the order without undue delay, and hence, the Directive imposes additional responsibilities on the service provider in Regulation 13 which deals with the liability of the service provider stipulating that: 'the duties imposed by regulations 6, 7, 8, 9(1) and 11(1) (a) shall be enforceable, at the suit of any recipient of a service, by an action against the service provider for damages for breach of statutory duty'[250].

Cooling off period

Most jurisdictions implement a combination of general and specific remedies aimed to protect consumer, and most provide for a 'cooling off' period during which the consumer can withdraw from a contract, under different laws, this period varies[251]. UK is no exception and the 'cooling off' period is provided for in The Consumer Protection (Distance Selling) Regulations 2000 which gave seven working days to the consumer 'from the day after the date of the contract, in the case of services, or from the day after the date of delivery of the goods' and 'where the supplier fails to comply with the information requirement at all, the cooling-off period is extended by 3 months'[252]. The Consumer Contracts Regulations of 2013 has amended the period from 7 to 14 days and cancellation period to 12 months in case of breach of information requirement[253]. The 'cooling off' period has further been extended by the Consumer Rights Act 2015[254] to 30 days[255].

New Rules Under Consumer Rights Act 2015 (The CRA)

The CRA sets a consolidating framework for the consumer rights in relation to contracts for supply of goods, services and digital content as well as the law related to unfair terms in consumer contracts. The main aim of the regulation is to provide a comprehensive legal instrument to both traders and consumers easy to use and integrated as it has been claimed that the UK consumer law 'was unnecessarily complex, fragmented and, in places, unclear for example, where the law had not kept up with technological change, lacked precision or was couched in legalistic language[256]. In general, the Act has consolidated provisions similar to already existing under various legal instruments,

[250] Ibid (197), Regulation 13
[251] S Corones, S Christensen, J Malbon, A Asher, J M Paterson, 'Comparative Analysis of Overseas Consumer Policy Frameworks' (2016) Queensland University of Technology accessed 15 February 2018 at http://consumerlaw.gov.au/files/2016/05/ACL_Comparative-analysis-overseas-consumer-policy-frameworks_Part1.pdf
[252] Ibid (205) (Explanatory note)
[253] Ibid (199), Section 30, 31
[254] Ibid (198), Section 22
[255] ibid
[256] P Giliker, 'The Consumer Rights Act 2015-A Bastion of European Consumer Rights?' (2016) *Legal Studies* Vol. 37 Issue 1, pp 78-102; As acknowledged by the government in its Explanatory Notes to the Act, at [5]

however, some changes have been introduced related to remedies availed in relation to defective goods, digital content and services.

In relation to goods, apart from the extended 'cooling off' period as discussed above, the consumer is now granted a right to a price reduction/refund or a final right to reject in case an adequate redress was not received by the consumer whether in a form of replacement or repair.

The most significant novelty introduced by the CRA are added provisions addressing digital content. It is the first legal instrument that regulates the supply of digital content, 'data which are produced and supplied in digital form'[257]. The provisions of the Act apply to digital content that is paid for and free content supplied along with other paid items. Similar to provisions related to goods, consumers are granted the right to receive a repair or replacement of the digital content or enjoy a price reduction.

In relation to obligatory information to be availed by the service provider to the consumer as provided for under the Consumer Contracts Regulations 2013[258], the CRA stipulates that such information will become a contractual term. Furthermore, a new right is incorporated in the CRA whereby a service provider makes certain information available prior to contracting, and the consumer takes this information into consideration, the service then must comply with such information[259].

The CRA is clearly a significant move towards a more confident and certain environment for e-commerce, and as Jo Swinson noted in his address: 'for too long consumers and businesses have struggled to understand the complicated rules that apply when buying goods and services…That is why the Consumer Rights Act is so important in setting out clear and updated consumer rights for goods, services and, for the first time, digital content…Well-informed, confident consumers are vital for driving continued growth and building a stronger economy'[260].

3.3.6 Jurisdiction

While, South Africa adopts an approach of dealing with the issue of jurisdiction as being vested on a South African court in a number of occasions[261], the UK legislation vests jurisdiction on English Courts where there exists one significant link with the domestic jurisdiction of England or Wales under the Computer Misuse Act 1990[262]. As ruled in *R v Waddon*[263] the content of US websites downloaded in the UK can fall under the jurisdiction of English courts.

However, the matters of electronic transactions are governed by existing rules of private international law[264] embedded with regards to disputes between EU consumers and traders within

[257] Ibid (248)
[258] Ibid (199)
[259] Ibid (248)
[260] Jo Swinson (then Consumer Minister) 'Biggest overhaul of consumer rights in a generation' Press Release 27 March 2015.
[261] Ibid (136) Section 90
[262] Computer Misuse Act 1990 Section 5
[263] *R v Waddon* (2000) All ER (D) 502 (CA).
[264] P Todd, *E-Commerce Law,* (Taylor and Francis, 2017)

the Rome Convention and Brussels Recast Regulation[265] which are 'technology-neutral' legislation instruments, with the broad intention to allow consumers to have their disputes under their home jurisdiction laws and courts of their country regardless of what the trader included in terms and conditions. However, the situation will vary from case to case depending on the circumstances and rules.

3.3.7 Cybercrime

The digital era and increased use of internet has transformed the market space and, hence, the way of the trade transactions with millions of consumers buying goods and services online. The UK taking a lion share of the European online shopping market[266], aims to ensure safety and confidence for the online consumers and traders which in turn are expected to support economic confidence, through enabling businesses to gain competitive advantage in the global market place securely developing new products and services, increasing volumes of business transacted securely online, instilling confidence in public service transactions among others[267]. The UK Government is constantly working on its legal framework to increase cyber security at all levels which is intended to serve strong basis for UK's engagement in international efforts 'to promote good internet governance'[268].

Offences committed using new technologies, such as offences against computer systems and electronic data, are dealt with in the Computer Misuse Act 1990[269].

Sections 1 and 2 of the CMA stipulate the following:

'(1) A person is guilty of an offence if-

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at-

(a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer'[270].

---

[265] REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

[266] 'Cyber Crime Strategy' (2010) Home Office, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, accessed 22 February 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

[267] ibid

[268] 'National Cyber Security Strategy 2016-2021' HM Government accessed 22 February 2018 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf

[269] Ibid (262)

[270] Ibid (262) Section1, 2

Under Section 1(a), an offence is committed by 'logging into or attempting to log into a computer system regardless of whether access is motivated by fraudulent intent or otherwise'[271]. Therefore, the crime herein is referred to as 'basic hacking'[272].

The CMA provides for illegal access in Article 2, for data interference in Article 4, for system interference in Article 5, for misuse of devices in Article 6; and in Section 1 for unauthorized access to computer material, Section 3 for an unauthorized acts and Section 3A covers making, supplying and obtaining articles for use.

The law provides for penalties in the form of fines and imprisonment.

As a general principle, under the UK law, legal persons can be held liable for criminal conduct due to their failure to exercise duty of care[273].

As mentioned earlier, jurisdictional matters are addressed in Sections 4-8 of the CMA, and in general provide for the 'significant links with domestic jurisdiction'. Further, the Serious Crime Act 2015[274] provides legal basis for prosecution of a UK national who commits offences as provided for under Sections 1-3A while outside the UK, 'where the offence has no other link to the UK, other than the offender's nationality'[275]. The extended extra-territorial jurisdiction applies to 'conspiracy or attempts to commit offences under the CMA'[276]. In relation to Section 3ZA of the Serious Crime Act, which provides the following:

'3ZA Unauthorised acts causing, or creating risk of, serious damage (1) A person is guilty of an offence if— (a) the person does any unauthorised act in relation to a computer; (b) at the time of doing the act the person knows that it is unauthorised; (c) the act causes, or creates a significant risk of, serious damage of a material kind; and (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused'[277], the following is considered a significant link with the domestic jurisdiction:

'(a) that the accused was in the home country concerned at the time when he did the unauthorised act (or caused it to be done);

(b) that the unauthorised act was done in relation to a computer in the home country concerned;

[271] O Omotubora, 'Comparative Perspectives on Cybercrime Legislation in Nigeria and the UK – A Case for Revisiting the "Hacking" Offences Under the Nigerian Cybercrime Act 2015' (2016) *EJLT* Vol 7 No 3
[272] ibid
[273] A Calder, *IT Governance: Guidelines for Directors* (IT Governance Ltd, 2005); Convention on Cybercrime Budapest, 23 November 2001 [The Convention entered into force for the United Kingdom on 1 September 2011]
[274] The Serious Crime Act 2015
[275] 'Computer Misuse Act 1990: Legal Guidance' accessed 22 February 2018 at https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990
[276] ibid
[277] Ibid Serious Crime Act

(c) that the unauthorised act caused, or created a significant risk of, serious damage of a material kind (within the meaning of that section) in the home country concerned'[278].

When it comes to common law, the jurisdiction of the court is fairly extensive, and where the offender had operated through a website hosted by a remote server in the US, the UK courts had jurisdiction to consider the case[279].
It is important to note that UK's cybercrime legislation is found not only in the CMA and the Serious Crime Act 2015, but in a range of different statutory instruments.

Lessons Learned

Taking into consideration rich regulatory landscape of the UK, Egypt is in the position to consider and study instruments regulating e-commerce as available under the laws of the UK as discussed in the section above. For instance, the UK rules are pretty detailed in terms of provisions guiding e-signatures and e-contracts; as well as its regulations dynamically updated regarding cybercrime and consumer protection aiming to grant maximum level of protection to the consumer might serve a good model to refer to. The UK legislation aims to employ a high standard in ensuring the security of data messages, set rules with regards to electronic contracts, and electronic signatures, as well as provide detailed guidance in relation to cybercrime. Furthermore, the UK presents a significant experience in amendment of existing laws such as CMA and Consumer Protection in order to bring these in line with the current technological trends and newly arisen obstacles in e-commerce. And this is reflective of the legislator's attempt at keeping pace with the technology, in view of its dynamic nature, which has this capability of rendering any legislation in this field outdated in a very short period of time. This approach is acclaimed and it is hoped that Egypt, the jurisdiction at focus of this thesis, takes a glance at the UK experience in light of the available legislation and its constant developments and perfections in this field. In other words, it is not only the existing legislation of the UK that should be looked at but rather its approach in legislation which is as dynamic as the changes in the field of e-commerce dictated by technological developments.

4. The Role of Cryptocurrencies and its Acceptance: Cross-Jurisdictional Approach with Special Emphasis on Egypt

Increasing importance in the realm of e-commerce is being gained by virtual currencies, whether the business is an online store or a bricks-and-mortar shop, if it accepts VCs such as Bitcoin, it needs to publicize that fact with a sign 'bitcoin accepted here'. As the main function of any currency is to serve the means of buying and selling goods, cryptocurrencies like bitcoin become frequently used for online e-commerce transactions with a growing number of businesses accepting digital currencies which offer low

[278] Ibid (204)
[279] *R. v Smith (Wallace and Duncan)* (No 4) [2004] EWCA Crim. 631, [2004] Q.B 1418. See also *R v Sheppard*and *R v Whittle* [2010] EWCA Crim. 65.

transactional fees and high speed of transactions. VCs have been gaining popularity in recent years with significant rise ratio in the digital age of today, linking the concept of money with advances in technology to 'challenge the traditional perceptions of currency and introduce alternatives that exist purely in digital form'[280].

According to the 'Global Cryptocurrency Benchmarking Study' of the University of Cambridge[281], the current number of 'unique active users of cryptocurrency wallets is estimated to be between 2.9 million and 5.8 million'[282]. The lines between different VC industry sectors are blurred with 31% of companies dealing with digital currencies are operating across 'two cryptocurrency industry sectors or more, giving rise to an increasing number of universal cryptocurrency companies'[283]. According to the same study, '79% of payment companies are engaged in relationships with banking institutions and payment networks', however, obtaining and maintaining such relationships are cited as one of the largest challenge of the sector. Further, it is being stated that 'on average, national-to-cryptocurrency payments constitute two-thirds of total payment company transaction volume, whereas national-to-national currency transfers and cryptocurrency-to-cryptocurrency payments account for 27% and 6%, respectively'[284].

According to the market dynamics, mostly fueled by a rapidly growing demand, the price of Bitcoin, for example, is determined by major exchanges, including Coinbase in San Francisco and Luxembourg's Bitstamp[285]. Bitcoin is fluctuating plunging from USD 11,000 to 9,300 and back to USD 10,000 reaching above USD 19,000 in December 2017. However, whatever the fluctuations are, the indicator is one-cryptocurrencies are in upward trend-with comparing indicators of USD 430 per Bitcoin in 2016, and USD 1 in 2011[286].

VCs' and in specific Bitcoin's worldwide spread has pushed governments and organizations to allow cryptocurrencies which have established themselves in international markets-from first ATM in Canada's Vancouver in 2013 to Dubai-based Aston Plaza and Residences which can be purchased through a Bitcoin payment[287].

---

[280] K McConnell, 'Best Practices for Bitcoins: Regulatory, Legal and Financial Approaches to Virtual Currencies in Hesitant, Global Environment' (2016) Thesis accessed 5 December 2017 at http://www.aph.gov.au/DocumentStore.ashx?id=46d34817-cdc7-42a5-97ec-e3ff59bd6634&subId=301945

[281] Dr. G Hileman, M Rauchs, 'Global Cryptocurrency Benchmarking Study' (2017) Cambridge Centre for Alternative Finance retrieved 5 December 2014 at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[282] ibid

[283] ibid

[284] ibid

[285] S Tarek, 'Egypt's Bitcoin Scene Seemingly Growing Despite Looming Uncertainties' (9 December 2017) Al Ahram Online retrieved 10 December 2017 at http://english.ahram.org.eg/NewsContent/3/12/282508/Business/Economy/Egypts-Bitcoin-scene-seemingly-growing-despite-loo.aspx

[286] ibid

[287] ibid

4.1 The Status of Cryptocurrencies in Egypt

With the rapid growth and novelty of cryptocurrencies, regulatory mechanisms on the legal arena are not yet precise and transparent. There is no consensus about how Bitcoin is defined, for example, or how it should be treated[288]. Until now, three regulatory approaches have developed in response to increasing popularity of Bitcoin: '1. To ban or severely restrict the use of Bitcoin; 2. Do nothing, issue warnings and 'wait and see' what action other countries take; 3. Take action and regulate virtual currencies'[289]. However, irrespective of the approach followed in a given jurisdiction, 'Bitcoin actors including intermediaries are still bound by general commercial, contractual and criminal laws'[290]. And as is being said, the case of Egypt is no different, where until now as we stand in the Year 2018, there are no special regulations governing cryptocurrencies in Egypt, and the provisions of the Civil Code and Commercial Code apply.

Apparently, the matter of sale of goods in Egyptian law is covered by two statutes: the Egyptian Civil Code[291] and the Commercial Code[292]. A brief comparison of Egyptian laws to the UK framework is provided herein.

The Civil Code provides a very similar definition to the one available under SGA[293] section 2(1) in its Article 418 whereby a 'sale is a contract whereby the vendor binds himself to transfer to the purchaser the ownership of a thing or any other propriety right in consideration of a price in money'[294]. The price is determined according to the Civil Code as follows:

Article 423[295]*:*

The method of establishing the price may be confined to the indication of the basis on which the price will be ultimately fixed.

When it is agreed that the price will be the market price, the market price will, in case of doubt, be that at the place where and at the time when the thing sold should be delivered to the purchaser; if there is no market at the place of delivery, reference should be made to the market price at the place at which the prices are customarily deemed applicable.

Article 424:

[288] Ibid (280)
[289] ibid
[290] R Bollen, 'The Legal Status of Online Currencies: Are Bitcoins the Future?' (December 2013), 24(4) Journal of Banking and Finance Law and Practice 272, 277
[291] Civil Code No. 131 of year 1948
[292] Commercial Code No. 17 of the year 1999
[293] Sale of Goods Act 1979
[294] Ibid (1) Art. 418
[295] Ibid (1)

When the contracting parties have not fixed a price for the thing sold the sale shall not be void if the circumstances show that the parties intended to adopt the current trade price or the price which they have usually applied in their dealings one with another.

These two provisions offer similarity to Section 8 of the SGA but in our case, is more elaborate. It is indicative as in Section 8 of SGA that the price can be fixed, but more elaborate in terms of determining the price as opposed to the 'reasonable price' determined by the facts offered by the SGA.

In terms of analyzing applicability of these provisions to the contemporary realities of e-commerce, there are two observations which can be made, which would definitely exclude cryptocurrencies, for example, or electronic commerce. One of them is direct reference to money as being 'the sum of money(s)' implying to currencies, and the other is found in Article 456[296]:

Article 456:

Subject to a clause or custom to the contrary, the price is payable at the place where the delivery of the thing sold is made.

If the price is not payable at the time of delivery of the thing sold, payment must be made at the domicile of the purchaser on due date.

This provision completely excludes newly available schemes of payment and delivery, in my point of view.

Now, these are the provisions of the Civil Code which apply to civil as well as commercial transactions. However, the Commercial Code governs all commercial transactions by default, and only in case, the conflict arising out of contract of sale of goods not covered by the Commercial Code will refer to the Civil Code provisions.

Now, the Commercial Code, Article 88[297] provides:

The provisions prescribed in this division shall apply to the goods sale contract, which are concluded between traders for trade-related matters unless otherwise prescribed by the law. These provisions shall not apply except when the charge in exchange for the sale is in cash, or both in cash and in kind, and the portion in kind is less than the portion in cash.

My concern here is referred to the 'portion of kind', the question is whether this is referring to the shares, for example, or might go as far as covering cryptocurrencies.

And, also, the law provides for determination of the price in Article 89[298]:

[296] Ibid (1) Art. 456
[297] Ibid (2) Art. 88
[298] Ibid Art. 89

1. If the contracting parties do not determine the price, the sale shall be concluded at the price on the basis of which dealings between them are concluded. If no previous dealings exist between them, the sale shall be concluded at the ruling price in the market.

2. If the agreement is reached on concluding the sale at the market price, or if the market price should be applied, according to the provision of the previous clause, the criterion shall be on the average market price at the time and place the contract is concluded. However, the foregoing shall only apply where nothing is otherwise agreed upon or the practice in trade provides differently, or if it transpires from the ruling conditions that another price must be applied. In case of multiple market prices, the criterion shall be on the medium price.

Now, looking and comparing the UK laws to Egyptian, I tend to come to a conclusion that there are not much of a difference except for more elaborate definitions in the Egyptian counterpart. And, the same question ponders with regards to Bitcoins, for example, if these would be covered under the Egyptian two Codes.

Furthermore, Egyptian laws governing securities do not provide coverage for the VCs, Capital Market Law[299], Civil Code[300], Commercial Code[301] and Companies Law[302] all deal with tangible securities either in the form of assets (movable and immovable), shares of the companies, or elsewise.

Talking about regulations and challenges associated with VCs[303], and in specific security issues and lack of regulatory base, practical exposure to the matter on the ground reveals the following (from my professional practice in the field).

Company A domiciled in USA and operating in the business of electronic currencies has been exposed to an attack by hackers from Egypt. Two Egyptians (17 and 18 years old) found a weak point in the electronic system of Company A and performed 123 transactions, by which they managed to illegally withdraw USD 50,000. The hackers had e-wallet accounts opened with Company A. Then, the money has been diverted to their accounts opened with other e-wallet providers, each of which received USD 10,000. At his point, Company A has requested legal support from Egypt.

The case has been rejected by several law firms in Egypt due to the absence of clear regulations governing the matter. My law firm has undertaken the challenge but when going deeper into the matter, it was realized that multiple jurisdictions were involved as the third-party providers were located in Russia, Cayman Islands, USA, Ukraine and other countries, where the stolen funds have been transferred to. Not to mention the

[299] Capital Market Law No. 95 of 1992
[300] No. 131 of year 1948
[301] Commercial Code No. 17 of the year 1999
[302] Companies Law No. 159 of 1981
[303] The Bitcoin ETF Will Be Rejected According to Prediction Markets' accessed 20 February 2017 at https://www.cryptocoinsnews.com/the-bitcoin-etf-will-be-rejected-according-to-prediction-markets/ ; The Bitcoin ETF Will Be Rejected According to Prediction Markets' accessed 20 February 2017 at https://www.cryptocoinsnews.com/the-bitcoin-etf-will-be-rejected-according-to-prediction-markets/

difficulty of locating IP, MAC addresses and other technicalities. Therefore, we had to work in both directions: law and cybernetics in order to come up with a proper legal brief and a case ready to go to the court. In our case, once the technical report was ready outlining the scheme of theft and electronic evidence, the claim was raised pertinent to the Penal Code[304] (theft) and Civil Code[305] (compensation). Most of the funds were returned prior to the court hearing as other e-wallet providers happened to freeze the accounts of the criminals and held the funds (without revealing such information to the Company A), the criminals were found. The rest of the stolen funds were returned, and the court released the judgment in favor of Company A and sentenced perpetrators to jail.

Given that the legal status of bitcoin differs from jurisdiction to jurisdiction and remains undefined[306], the question arises as to how to deal with the realities and real cases happening on the ground specifically when it comes to security and cross-border transactions. While some countries allowed the use and trade, other have restricted. The question arises as to how to deal with insecurities and definitions when handling cases related to digital currencies.

Leaving security issues apart and talking about definitions, consider the following: 'while the SEC asserts that bitcoin mining contracts are securities, the FBI has declared Bitcoin as "property" while FinCEN seems to be regulating it as a currency'[307].

It is clear that the existing complexity and confusion calls for the proper legislative measures on international arena with regards to Bitcoin regulation which has to be coordinated between governments and financial institutions.

In December 2017, the Central Bank of Egypt (CBE), has refuted speculation that Bitcoin platform will officially be established and further declared that it will not regulate digital currency dealings as 'the virtual currency is not guaranteed by the banking sector […] and dealing with is the responsibility of its users', according to the CBE statement[308]. And this is not surprising as Egypt has not followed other countries, which even in the lack of regulations are considered to be VCs-friendly such as Japan and Sweden, nor did Egypt follow Bolivia and Bangladesh, where cryptocurrency trading is banned[309].

Bitcoin trading in Egypt is not legalized, yet it is not illegal. And although, the punishment for trading currency in the Egyptian black market has been intensified since 2016, with the imprisonment extended from no more than three months to three years, transactions involving cryptocurrencies are not explicitly addressed. According to Rostom Omar, an Egyptian lawyer, 'If there is no law, there is no crime, and we don't have laws that might apply to Bitcoin […] Bitcoin is virtual, does not have an official

[304] Penal Code 58/1937 and its Amendments
[305] Civil Code 131/1948
[306] I Demartino, 'Bitcoin Regulation: SEO Calls Mining Contracts 'Securities'' (2016) accessed 20 February 2017 at http://coinjournal.net/bitcoin-regulation-sec-calls-mining-contracts-securities/
[307] ibid
[308] Ibid (285)
[309] ibid

exchange rate in Egypt and not even accredited as a currency by the state authorities. Therefore, criminalizing any Bitcoin activities would be very difficult'[310].

In line with the state policy, Egypt's authorities could either regulate Bitcoin and impose profit sharing from Bitcoin trade or ban it completely with the aim to force traders in cryptocurrencies to switch their funds to the official economy[311]. However, at present it remains unclear whether Egypt will pursue one of the above options or would yet select to maintain the 'status-quo'. At present, according to the governor of the CBE, Tarek Amer, the CBE is trying to find a strategy in terms of the direction of dealing with financial technology and associated risks[312].

Meanwhile, on the 31st of December 2017, Dar Al-Ifta Al Missriyyah, an institute responsible for issuing fatwa (religious verdicts/rulings) affiliated as a division of Egypt's Ministry of Justice[313], issued a fatwa that deems virtual currencies as forbidden by Islam[314].

Mufti Councilor Magdy Ashour, based his Islamic ruling on an assumption that Bitcoin is being used for funding terrorism, and on the fact that virtual currencies are not covered by the Central Bank of Egypt (CBE). Moreover, according to him, a transaction of funds is a contractual relationship with set rules, and since cryptocurrencies do not fall under such, Islam will consider such currencies as forbidden[315]. The Egyptian Grand Mufti, in

[310] ibid
[311] ibid
[312] ibid
[313] http://www.dar-alifta.gov.eg/Foreign/default.aspx?LangID=2&Home=1

Adopted from official website: [Dar al-Ifta al Misriyyah is considered among the pioneering foundations for fatwa [Religious verdicts] in the Islamic world. It was established in 1895 by the high command of Khedive Abbas Hilmi, and was affiliated to the Ministry of Justice on 21st November, 1895 by Decree No. 10. Since it was first established, Dar al-Ifta al-Misriyyah has been the premier institute to represent Islam and the international flagship for Islamic legal research. It fulfills its historic and civil role by keeping contemporary Muslims in touch with religious principles, clarifying the right way, removing doubts concerning religious and worldly life, and revealing religious laws for new issues of contemporary life.

Dar al-Ifta al Misriyyah is among the pillars of the religious foundations in Egypt which include Al-Azhar Al-Sharif, Al-Azhar University, Ministry of Religious Endowments, and Dar al-Ifta al-Misryyah. It plays a significant role in giving rulings to the masses and consultation for the judiciary in Egypt. Dar al-Ifta al Misryyah started as one of the divisions of the Egyptian Ministry of Justice. In view of its consultancy role, capital punishment sentences among others are referred to the Dar al-Ifta al-Misryyah seeking the opinion of the Grand Mufti concerning these punishments. The role of Dar al-Ifta does not stop at this point; it is not limited by domestic boundaries but extends beyond Egypt covering the entire Islamic world.

This leading role is best expressed by its records of fatawa from its inception until the present day. Dar al-Ifta receives inquiries from all over the Islamic world, as well as foreign students of Islamic law for training. This leadership developed from Dar al-Ifta's role as scholarly reference and for adopting a moderate methodology in understanding rulings derived from the inherited Fiqh (Eng. Jurisprudence) creating a consistency between Islamic law and the needs of the society].

[314] http://www.egyptindependent.com/egypts-dar-al-iftaa-deems-bitcoin-currency-forbidden-islam/; https://www.rt.com/business/414903-egypt-mufti-ban-bitcoin/
[315] ibid

his commentary, noted that 'trade in cryptocurrency is similar to gambling, which is forbidden in Islam'[316] 'due to its direct responsibility in financial ruin for individuals'[317]. And hence, it was explained that Bitcoin could have a negative impact on the legal safety of traders and lead to an 'ease in money laundering and contrabands trade'[318]. Mufti also noted, that Egypt's legitimate entities do not recognize trade in VCs as acceptable and that such use of VCs 'impinges on the state's authority in preserving currency exchange'[319].

Keeping in mind that Egypt's legal system is codal in nature and 'the principles of Islamic Sharia are the principle source of legislation'[320], following the fatwa banning cryptocurrencies (dated 31st December 2017) it is foreseeable that future legislation, if any, will outlaw cryptocurrencies as the code/legislation that is to come shall not contradict the principles of Sharia.

Egypt is not the only jurisdiction that is struggling the struggle, attitude to the matter isn't much different in Canada for example, where according to Carolyn Wilkins, Bank of Canada senior deputy governor, 'central-bank issued currencies play a significant role in financial stability and function as a 'transmission mechanism for monetary policy'[321]. However, according to the same source, the central bank initiatives are not likely to push out the 'private alternatives'[322]. Given the nature of traded currencies such as bitcoins[323] and its novelty it is important to point out that regulatory system is not yet adapted to accommodate the nature of such e-dealings as well as ensure security. According to the authors[324], a 'well designed and managed private currencies could circulate widely but only with appropriate government regulation to ensure their safety, soundness and uniformity'[325].

4.2 Current Legal Regulatory Framework in South Africa

South Africa being among advanced economies, is yet lagging in development of regulations governing cryptocurrencies. The current stance on the matter is pretty much similar to that of Egypt. Until now, there is no legislation promulgated regulating cryptocurrencies[326]. There was no public consultation through which Parliament consults

[316] https://www.rt.com/business/414903-egypt-mufti-ban-bitcoin/
[317] ibid
[318] ibid
[319] ibid
[320] Article 2, Egypt's Constitution 2014
[321] 'Bank of Canada: Digital Currencies Need Regulation to Grow' accessed 20 February 2017 at https://www.cryptocoinsnews.com/bank-canada-digital-currencies-need-regulation-grow/
[322] ibid
[323] Ibid
[324] Ibid
[325] ibid
[326] D Raviv, 'Is Bitcoin Legal in South Africa?' (2016) GoLegal Industry News and Insights, accessed 24 December 2017 at https://www.golegal.co.za/bitcoin-legal-south-africa/ ; M S Wicht, 'The Tax Implications of Bitcoin in South Africa' (2016) LLM Thesis, University of Pretoria accessed 24 December 2017 at https://repository.up.ac.za/bitstream/handle/2263/60114/Wicht_Tax_2017.pdf?sequence=1&isAllowed=y

with interested or affected entities, and hence, no legal protection is granted to traders of Bitcoin in South Africa[327].

The South African National Treasury on behalf of the South African Reserve Bank (SARB), the Financial Services Board (FSB), the South African Revenue Services (SARS) and the Financial Intelligence Center, have warned users of Bitcoin in the alert issued 18 September 2014[328], of the risks associated with digital currency transactions such as lack of security, convertibility[329] and value, additionally, the alert provided a definition of a virtual currency[330]. The SARB further warned that it does not regulate or supervise cryptocurrencies' landscape, and hence, all activities associated with trade and/or use of VCs are at the sole discretion and liability of a user with no recourse to the bank[331].

According to the South African Reserve Bank Act[332], SARB has the sole right to manage currency and issue coins and notes (Legal Tender), Bitcoin, however, falls outside the definition of a legal tender[333]. Moreover, VCs are not covered by the Financial Markets Act 2012[334] and, hence, do not fall under the definition of securities[335].

---

[327] A Nieman, 'A Few South African Cents' Worth Bitcoin' (2015) 18(5) *Potchefstroom Electronic Journal* 1979

[328] South Africa, The Department of National Treasury, 2014, User Alert: Monitoring of Virtual Currencies

[329] The Financial Action Task Force (FATF) defined virtual currency in its paper Virtual Currencies Key Definitions and Potential AML/CFT Risks Report: '(a) all non-convertible virtual currencies are centralized to a particular virtual community and cannot be exchanged for real currency; (b) convertible virtual currencies have an equivalent value in real currency and can be exchanged back and forth for a real currency. Convertible virtual currencies may be either centralized or decentralized: (i) centralized convertible currencies have a single third-party administering authority, who functions as a neutral entity between the principals in a transaction, and who controls the system. This administrator issues the currency, establishes the rules for its use, maintains a central payment ledger and has authority to redeem the currency; (ii) decentralized convertible virtual currencies are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring oversight. Examples of decentralized convertible virtual currencies include Bitcoin'

[330] 'A virtual currency is a unit of account that is digitally or electronically created and stored. Members of the virtual community agree to accept these units as a representation of value in the same way that currency is accepted. In contrast to traditional currencies, virtual currencies operate without the authority of central banks, and are therefore not regulated. An example of virtual currency is Bitcoin…[which] is software based and uses peer-to-peer technology to operate without the involvement of the central bank or commercial banks'

[331] Commonwealth, Financial Action Task Force, (2014) '*Virtual Currencies: Key Definitions and Potential AML/CFT Risks*': '(a) the lack of proper regulatory and legal framework substantially exacerbates risks associated with the enforcement of the principle of finality and irrevocability in the payment system; (b) there is no regulatory protection that would compensate the owner or user of virtual currencies for any loss that may be suffered; (c) virtual currencies are less susceptible to freezing or seizure actions by law enforcement agencies. The identification of relevant laws applicable to the contravention and the gathering of evidence regarding a transaction can become am unattainable task; (d) the transfer of virtual currencies in and out of SA is not governed by exchange regulations. Any cross-border exchange can therefore not be authorized by SARB'.

[332] Act No. 90 of 1989

[333] Ibid (326)

[334] Act No. 19 of 2012

[335] Ibid, Section 1: '(a) listed and unlisted-(i) shares, depository receipts and other equivalent equities in public companies, other than shares in a share block company as defined in the Share Blocks Control Act 59 of 1980; (ii) debentures, and bonds issued by public companies, public state-owned enterprises, the South African Reserve Bank and the Governments of the Republic of South Africa; (iii) derivative instruments; (iv) notes; (v) participatory interests in a collective investment scheme as defined in the Collective Investment Schemes Control Act 45 of 2002 and units or any other form of participation in a foreign collective investment scheme approved by the Registrar of Collective Investment Schemes in terms of section 65 of that Act; and (vi) instruments based on an index; (b) units or any other

In 2017, South Africa is taking significant steps towards creating a regulatory framework for VCs. SARB has recently announced that it intends to test regulations pertaining to digital currencies. Further, in February 2017, SARB announced that it is intending to create a national virtual currency based on distributed ledger technology as well as adopt cryptocurrencies and blockchain within South Africa[336]. Moreover, the National Treasury along with the SARB, FIC, and FSB have established an Intergovernmental Fintech Working Group in December 2016, in order to develop an approach and potential policy regulating fintech including VCs, and to deal with crowdfunding, robo-advice, and alternate payment platforms[337]. Minister of Finance, Gigaba announced that a 'balanced approach is being taken' to the development of bitcoin and cryptocurrency regulations. He further stated that the government aims to develop a 'juridical apparatus that is supportive of the objectives of enhances innovation, competition and financial inclusion in the financial sector, while also reviewing risks related to financial customer protection, money laundering and financial stability.'[338]

4.3 The Approach in the UK

UK is hosting Bitcoin products and services as well as operating cryptocurrency exchanges[339], however, regulation of cryptocurrencies and its trade has been left unacknowledged as is the case in many other jurisdictions. However, there are three main regulatory areas which shall be considered when discussing cryptocurrency trading in the UK: consumer protection, money laundering prevention, and taxation[340].

The Financial Conduct Authority (FCA)[341], the regulator responsible for ensuring of consumer protection and integrity of the market during provision of financial services, does not provide any guidance in relation to regulation of VCs. It further stated that it does not regulate digital currencies and has no intention of doing so[342]. Therefore, there is no obligation for digital currency businesses to register with or obtain authorization from the FCA.

Another aspect is the prevention of money laundering, which is approached seriously by the UK, where the Money Laundering Regulations 2017[343] are enforced by the Tax Authority, HM Revenue and Customs, the FCA, as well as other entities. However, there

---

form of participation in a collective investment scheme licensed or registered in a country other than the Republic; (c) the securities contemplated in paragraphs (a)(i) to (vi) and (b) that are listed on an external exchange; (d) an instrument similar to one or more of the securities contemplated in paragraphs (a) to (c) prescribed by the registrar to be a security for the purposes of this Act'

[336] https://news.bitcoin.com/south-africa-will-begin-testing-bitcoin-and-cryptocurrency-regulations/

[337] https://news.bitcoin.com/south-africa-to-take-balanced-approach-to-bitcoin-and-cryptocurrency-regulations/

[338] ibid

[339] https://www.buybitcoinworldwide.com/united-kingdom/ accessed 7 January 2018

[340] E Jankelewitz, 'Bitcoin Regulation in the UK' (2014) accessed 7 January 2018 at https://www.coindesk.com/bitcoin-regulation-uk/

[341] https://www.fca.org.uk/

[342] Ibid (340)

[343] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

are no formal obligations related to prevention of money laundering through trade in digital currencies.

Given the evolutionary nature of the VCs and the legal and regulatory environments they are operating in, HM Revenue and Customs (HMRC), has issued a policy paper addressing the matter of Value Added Tax treatment of Bitcoin[344]noting that these provisions[345] 'in no way reflects on how they are treated for regulatory or other purposes'[346].

As in many other jurisdictions, there are extensive efforts being undertaken in an attempt to regulate cryptocurrencies, and the UK is no exception. The British Treasury is planning to introduce regulations that would treat Bitcoin and other VCs in 2018[347]. The Treasury said: 'We are working to address concerns about the use of cryptocurrencies by negotiating to bring virtual currency exchange platforms and some wallet providers within anti-money laundering and counter-terrorist financing regulation'[348].

The foreseen legislation is intended to embrace entire EU and oblige digital currency traders to abide by identity disclosure rules and suspicious activity reporting when dealing with VCs. It is also expected that EU member states will introduce specific digital currency-related laws and regulations affecting businesses and individuals[349].

4.4 Conclusion

As is evident from above comparison of three selected jurisdictions, regulators and law makers worldwide are concerned with the development of proper legal frameworks which would provide legal guidance for traders in digital currencies. As was noted in the

[344] Revenue and Customs Brief 9 (2014): Bitcoin and other Cryptocurrencies issued 3 March 2014 accessed 7 January 2018 at https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies

[345] a) income received from Bitcoin mining activities will generally be outside the scope of VAT on the basis that the activity does not constitute an economic activity for VAT purposes because there is an insufficient link between any services provided and any consideration received; b) income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of 'transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments'; c) when Bitcoin is exchanged for Sterling or for foreign currencies, such as Euros or Dollars, no VAT will be due on the value of the Bitcoins themselves; d) charges (in whatever form) made over and above the value of the Bitcoin for arranging or carrying out any transactions in Bitcoin will be exempt from VAT under Article 135(1)(d) as outlined at 2 above.

[346] Ibid (344)

[347] J Kollewe, 'Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears' (December 2017) The Guardian accessed 7 January 2018 at https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity ; https://cointelegraph.com/news/british-treasury-plans-to-implement-eu-wide-cryptocurrency-regulation-by-late-2018

[348] ibid

[349] https://cointelegraph.com/news/british-treasury-plans-to-implement-eu-wide-cryptocurrency-regulation-by-late-2018

report by the UK Government Chief Scientific Adviser[350] regulation of an unpermissioned system[351] such as Bitcoin by means of legal code is a complicated matter as there is no single entity in control of the system[352], and therefore, emphasis in relation to regulation of Bitcoin as well as other VCs is placed on developing legal codes which would regulate businesses that deal and trade with Bitcoin such as exchanges and electronic wallet providers. An example of regulation of money transmission businesses via legal instrument is found in the US where BitLicense issued by the New York State Department of Financial Services must be obtained by businesses offering digital currency services to the residents of New York[353].

5. Conclusions and Guidelines for Egypt-Proposals for Reform

With the enactment of E-Signature Law No. 15/2004 of Egypt, Egypt has stepped towards a legal framework for e-commerce. However, it still has a long way to go before the goal of attaining a sound legal framework is realized. E-Signature Law of Egypt represents a non-comprehensive tool which as discussed in the course of the thesis does not cover the majority of fields related to e-commerce, and hence, Egypt should implement e-commerce contractual rules pertaining to automated contracts, attribution, acknowledgement of receipt, time and place a message is assumed to have been sent and received, carriage contracts[354], cybercrime and consumer protection of consumers concluding electronic transactions with online traders. Taking into consideration provisions and legislative instruments available in the UK and South Africa, as discussed in this thesis Egypt might benefit and come out with tailored and detailed provisions covering each of the loopholes as mentioned above.

While creating additional e-commerce contractual rules, Egypt should seek to comply and benefit from additional requirements from jurisdictions such as South Africa and the UK. It is clear that Egyptian statute is way less thorough than UK's and South Africa's legislative instruments, as E-Signature Law deals with statutory requirements pertaining

[350] 'Distributed Ledger Technology: Beyond Block Chain' (2016) HM Government Office for Science accessed 7 January 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[351] Unpermissioned ledgers such as Bitcoin have no single owner — indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state. Unpermissioned ledgers can be used as a global record that cannot be edited: for declaring a last will and testament, for example, or assigning property ownership. But they also pose a challenge to institutional power structures and existing industries, and this may warrant a policy response.

[352] Ibid (350)

[353] New York Department of Financial Services 'BitLicense Regulatory Framework'. Available at http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework. htm

[354] Ibid (67)

to writing and signing, and Draft E-Commerce law is very much general and does not address important aspects of e-commerce dictated by technological advancements.

Comparing the E-signature provisions of the UK, South Africa and Egypt, the statutes of the UK and South Africa present provisions and requirements which are not covered in the Egypt's statute. For example, the UK implements a three-tier system recognizing electronic signature, advanced electronic signature and qualified electronic signature and provides for '(1) In any legal proceedings— a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data. (2) For the purposes of this section an electronic signature is so much of anything in electronic form as— (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and (b) purports to be used by the individual creating it to sign.'[355] Moreover, UK regulation recognizes and provides for electronic seals and related certificates, electronic time stamps and related certificates, electronic documents and related certificates, electronic registered delivery service and related certificates. South Africa's ECTA adopts two-tier system recognizing electronic signatures as 'a facility for legal assurance in electronic commerce'[356] by treating e-signatures as a functional equivalent of handwritten signatures for the purpose of electronic transactions. The ECTA identifies two types of e-signatures: a) an 'electronic signature' defined as 'data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'[357]; and b) 'advanced electronic signature', 'AeS', defined as 'an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37'[358]. These rules, which are pertinent to compliance with other statutory requirements, should be added to the Egyptian legislative instruments. More specifically, Egypt should consider adopting statutory language from other jurisdictions such as the UK and South Africa discussed herein.

Another facet which can be taken into consideration by the Egyptian legislator, as suggested by Forder[359], 'would be to establish and enhance the rating of signature activity'[360] whereby certain guidelines are to be provided suggesting which methods are to be considered valid and admissible for particular legal purposes for a signature. This could be market-driven activity regulated by the competent authorities; whereby ultimately the rating would enhance certainty and predictability for the user of e-signatures.

[355] Ibid (203) Schedule 3
[356] R Low, S Christensen, 'E-signatures and PKI Frameworks in Australia.' (2004) *The Digital Evidence Journal, incorporating the e-Signature Law Journal* 1(2): pp. 56-59.
[357] ECTA, Chapter 1, Section 1
[358] ibid
[359] J Forder, 'The Inadequate Legislative Response to E-signatures' (2010) 26 *Computer Law and Security Review* 418
[360] Ibid (211)

Further flaw in the Egyptian legislation is its failure to address consumer protection for e-commerce consumers as well as stipulate obligations for online traders. As a model, Egypt can take the UK and/or South Africa's legislative instruments which offer consumer protection for its e-commerce buyers. Provisions of both 'model' laws provide consumers with a last chance to review the order before concluding the transaction as well as 'cooling off' period during which a transaction can be cancelled. The UK law further avails rights to refund in case the goods are not delivered or do not conform to specifications.

Beyond the provisions discussed above, cyber crimes' provisions under Egyptian law, or in particular their lack represents another flaw. As the internet offers the potential for a criminal to commit offences across the borders this poses a challenge for traditional law enforcement, even at national levels, as the offences can be committed against individuals in various countries at the same time. This factor presents not only a challenge to legislators, vacuum in the legislative space with this regard instills insecurities and hence, hinder e-commerce activities in a given jurisdiction, such as Egypt, for example, which does not have specific legislation dealing with cybercrime. Cyber offenders commonly seek to exploit weaknesses of jurisdictions' legislation by committing crimes in one country and delivering their effect in another jurisdiction. 'In deliberately targeting their activities in or through jurisdictions where regulation or legislation is not strong, or where investigative or other co-operation is known to be poor, cyber criminals can minimize the risk of their activities being discovered or punishment being effected'[361].

And hence, Egypt should address cybercrime in more details, and similar to South Africa's legislation and the UK laws, should address the following computer crimes and introduce appropriate penalties: '1. Unauthorized tampering with computer information; 2. Unauthorized use of a computer service; 3. Unauthorized interference in the operation of a computer; 4. Unauthorized dissemination of computer access codes or passwords; and 5. Injection of a virus into a computer.'[362]

The UK's CMA and Serious Crime Act 2015 can be used as a model for such additions.

Furthermore, looking into the e-government angle of the matter, in order to make regulations stronger, e-government provisions within the E-Signature Law or any other legislative instrument in perspective should be strengthened. In current shape, the provisions are 'relatively weak because they are permissive' whereas they should be mandatory[363]. Egypt should consider integrating an advanced computer information system within governmental departments, as well as introducing enabling regulations in order to facilitate provision of e-government services to the public as Egypt is witnessing high rates of internet users. UK might serve as an example of a jurisdiction which is on

[361] Ibid (266)
[362] Ibid (67)
[363] Ibid

its way of successful implementation of e-government which now makes a substantial number of government services accessible online.

The matter of jurisdiction is another important aspect which currently remains unaddressed by the Egyptian legislation. In order to give future regulations full weight, Egypt should consider the trans-border nature of e-commerce transactions and make its legal instruments applicable to the foreign individuals or entities whose actions have an effect on Egypt by virtue of transmission of an electronic message received in Egypt. Thus, the foreign party shall be prevented from evading the jurisdiction of Egyptian courts due to the mere fact of this party not being physically present in Egypt.

On the final note, cryptocurrency and its recognition remain the focus of international debate including South Africa and the UK. Egypt, shall definitely participate and follow the discussions in order to ensure timely introduction of proper legislative tools in order to follow the international e-trade patterns and regulations.

To conclude, given the rapid technological advances in the area of e-commerce, it is essential for Egyptian legislators to identify and adopt the best international practices in this dynamic field in order to boost its economic growth, increase digital trade and instill certainty and predictability for both e-commerce consumers and online traders. Egypt's legislators should move beyond mere legal recognition of electronic signatures and address vital issues as discussed above, resolution of which are crucial in terms of removal of major obstacles in the field of e-commerce. Examination of Egypt's legislation and its comparison to other jurisdictions revealed that Egypt's current legal regime remains highly underdeveloped and ineffective in regulating e-commerce activities. While South Africa and the UK, present encouraging legislative models and qualify as viable tools for the regulation of e-commerce activities, Egypt has a long way to go and is encouraged to take these into consideration.

On the final note, it is suggested that Egyptian legislators charged with the duty of creating legal instruments need to keep the pulse and remain abreast of developments in the area of e-commerce in other jurisdictions in order to ensure further development of a more advanced and secure legal framework for the ever-flourishing e-commerce.

6. Bibliography

6.1 Legislation

Egypt

Capital Market Law No. 95 of 1992

Civil Code No. 131 of year 1948

Commercial Code No. 17 of the year 1999

Companies Law No. 159 of 1981

Decree No. 209 of the year 2000 of the Minister of Communications and Information Technology

Decree No. 109 of the year 2005 issuing Executive Regulation of E-Signature Law No. 15/2004

Egypt's Constitution 2014

'Egypt: Draft Law on E-Commerce' (2001) Vol. 16 No. 3 *Arab Law Quarterly* 288-294 retrieved from https://www.jstor.org/stable/3382177?seq=1#page_scan_tab_contents

Law 15 of 2004 on E-Signature

Law No 88/2003 promulgating the Law of Central Bank of Egypt

Ministerial Decree No. 2 of 1999 issued by the Ministry of Trade and Supply to formulate a committee to develop the electronic commerce legislation

Penal Code 58/1937 and its Amendments

The Central Bank of Egypt (CBE) Decision (14 April 2011)

The Central Bank of Egypt (CBE) Decision (2 February 2010)

United Kingdom

Computer Misuse Act 1990

Consumer Rights Act 2015

Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (2016 No.696) (The Regulation (EU) No 910/2014 (the 'eIDAS Regulation')

Electronic Communication Act 2000

Electronic Signatures Regulations 2002 No. 318

Sale of Goods Act 1979

The Consumer Protection (Distance Selling) Regulations 2000 No. 2334

The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 No. 3134

The Data Protection Act 1998

The Electronic Commerce (EC Directive) Regulations 2002 No. 2013

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

The Privacy and Electronic Communications (EC Directive) Regulations 2003 No. 2426

The Serious Crime Act 2015

South Africa

Act No. 90 of 1989

Act No. 19 of 2012

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

Other

Directive 1999/93 of the European Parliament and Council on a Community Framework for Electronic Signatures

'Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)', contained in Model Law (Objectives No. 5)

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the *"eIDAS Regulation"*)

REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

UNCITRAL Model Law on Electronic Commerce with Guide Enactment 1996 with additional article 5 bis as adopted in 1998 accessed 8 October 2017 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998 accessed 8 October 2017 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

United Nations Convention on the Use of Electronic Communications in International Contracts accessed 8 October 2017 at http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (New York, 2008) (the "Rotterdam Rules") http://www.uncitral.org/uncitral/en/uncitral_texts/transport_goods/2008rotterdam_rules.html

6.2 Case Law

Bennet v Brumfitt [1867-1868] LR 3 CP 28

Golden Ocean Group v Salgaocar Mining Industries [2011] EWHC 56 (Comm)

Grainger & Sons v Gough (1896) AC 325, 334

Jenkins v Gaisford [1863] 3 Sw & T 93

Mehta v J Pereira Fernandes SA [2006] EWHC 813

Newborne v Sensolid [1954] 1 QB 45; *Godwin v Francis* [1870] LR 5 CP 295

Partridge v Crittenden (1968) 2 All ER 421

Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd (1953) 1 QB 401

R. v Smith (Wallace and Duncan) (No 4) [2004] EWCA Crim. 631, [2004] Q.B 1418.

*R v Sheppard*and *R v Whittle* [2010] EWCA Crim. 65.

R v Waddon (2000) All ER (D) 502 (CA)

Spencer v Harding (1870) LR 5 CP 561

6.3 References

A A Alajaji, ‘An Evaluation of E-Commerce Legislation in GCC States: Lessons and Principles from the International Best Practices (EU, UK, UNCITRAL)’ (2016) Submitted for the degree of Doctor of Philosophy

A Calder, *IT Governance: Guidelines for Directors* (IT Governance Ltd, 2005); Convention on Cybercrime Budapest, 23 November 2001 [The Convention entered into force for the United Kingdom on 1 September 2011]

A J Mambi, *ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community* (African Books Collective, 2010) 172f

A Nieman, 'A Few South African Cents' Worth Bitcoin' (2015) 18(5) *Potchefstroom Electronic Journal* 1979

B H. Malkawi, 'E-commerce in Light of International Trade Agreements: The WTO and the United Sstates-Jordan Free Agreement', (Summer 2007), *International Journal of Law and Information Technology*

'Bank of Canada: Digital Currencies Need Regulation to Grow' accessed 20 February 2017 at https://www.cryptocoinsnews.com/bank-canada-digital-currencies-need-regulation-grow/

C Erasmus, 'Consumer Protection in International Electronic Contracts' (2011) Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Magister Legum* in Import and Export Law at the Potchefstroom campus of the North-West University.

Commonwealth, Financial Action Task Force, (2014) '*Virtual Currencies: Key Definitions and Potential AML/CFT Risks'*

'Consumer Protection in Electronic Commerce' (2017) United Nations Conference on Trade and Development (UNCTAD), TD/B/C.I/CPLP/7 accessed 26 November 2017 at http://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf

'Computer Misuse Act 1990: Legal Guidance' accessed 22 February 2018 at https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990

'Cyber Crime Strategy' (2010) Home Office, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, accessed 22 February 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

'Distributed Ledger Technology: Beyond Block Chain' (2016) HM Government Office for Science accessed 7 January 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Dr. G Hileman, M Rauchs, 'Global Cryptocurrency Benchmarking Study' (2017) Cambridge Centre for Alternative Finance retrieved 5 December 2014 at

https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

D Raviv, 'Is Bitcoin Legal in South Africa?' (2016) GoLegal Industry News and Insights, accessed 24 December 2017 at https://www.golegal.co.za/bitcoin-legal-south-africa/

D Ruvic, 'Bitcoin Banned by Islam': Egypt's Grand Mufti Issues Fatwa Against Cryptocurrency' (2018) accessed at https://www.rt.com/business/414903-egypt-mufti-ban-bitcoin/

E Jankelewitz, 'Bitcoin Regulation in the UK' (2014) accessed 7 January 2018 at https://www.coindesk.com/bitcoin-regulation-uk/

Economist Intelligence Unit, *Egypt: Overview ofE-Commerce*, GLOBAL TECH. F. (Aug. 3, 2007), http://globaltechforum.eiu.com/index.asp?layout=printer-friendly&doc-id=11174.

'Egypt Poised to Accelerate E-commerce Growth with New National Strategy' (20 March 2017) accessed 29 October 2017 at http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1453

'Electronic Signatures and Trust Services Guide' Department for Business, Energy, and Industrial Strategy accessed 20 February 2018 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/bis-16-15-electronic-signatures-guidance.pdf

'Executing a Document Using Electronic Signature' (2017) HM Registry accessed 20 February 2018 at https://hmlandregistry.blog.gov.uk/2017/02/08/executing-document-electronic-signature/

F Amereller, K Balz, S Klaiber, 'A Guide to Business Law in Egypt' (2010) accessed 10 December 2017 at http://amereller.com/wp-content/uploads/2016/10/Amereller_Egypt-Guide-2010.pdf

F F Wang, 'The Incorporation of Terms into Commercial Contracts: A Reassessment in the Digital Age' (2015) *Journal of Business Law*

Financial Conduct Authority Official Website accessed at https://www.fca.org.uk/

F Sudweeks, C.T. Romm, 'Introduction' In *Doing Business on the Internet: Opportunities and Pitfalls*, (London: Springer-Verlag: 1-7, 1999)

F Tasneem, 'Enforceability of Electronic Contracts in Australia' (2015) RMT University

F Tawfeek, 'Egypt's Dar al-Iftaa Deems Bitcoin Currency as Forbidden in Islam' (2018) accessed http://www.egyptindependent.com/egypts-dar-al-iftaa-deems-bitcoin-currency-forbidden-islam/

G Gilmore, 'On the Difficulties of Codifying Commercial Law' (1948) 57 *Yale LJ* 1341.

H Huffmann, 'Consumer Protection in E-Commerce: An Examination and Comparison of the Regulations in the European Union, Germany and South Africa that Have to Be Met in Order to Run Internet Services and in Particular Online Shops' (2004) LL.M Thesis, University of Cape Town accessed 10 October 2017 at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.7671&rep=rep1&type=pdf

http://isdo-hwahab/isdo/Esignature.asp and also http://www.mcit.gov.eg/proj_link.asp, last visited on 28
June 2004.

https://www.buybitcoinworldwide.com/united-kingdom/

H El-Mahdaw, 'Is the Government Watching Egyptians or Watching Over Them: Egypt's Cyber Crime Law in January' (Tuesday, 3 January, 2017) Ahram Online accessed 18 February 2018 at http://english.ahram.org.eg/NewsContent/1/64/253973/Egypt/Politics-/Is-the-government-watching-Egyptians-or-watching-o.aspx

I Demartino, 'Bitcoin Regulation: SEO Calls Mining Contracts 'Securities''' (2016) accessed 20 February 2017 at http://coinjournal.net/bitcoin-regulation-sec-calls-mining-contracts-securities/

I Elbeltagi, *'E-Commerce and Globalization: An Exploratory Study of Egypt' (2007),* 14:3 *CROSS-CULTURAL MGMT: AN INT'L J.,* 196, 196-201

I J Lloyd, *Information Technology Law* (6th edn, Oxford University Press 2011)

'Introduction to E-Commerce', LINKEGYPT, http://www.linkegypt.com/blogs/b/Introduction-to-ecommerce/22/Introduction-to-ecommerce.htmI (last visited Apr. 2, 2011)

'Internet users in Egypt hit 33M in April 2017' Egypt Today, August 21, 2017 accessed 15 October 2017 at https://www.egypttoday.com/Article/1/18486/Internet-users-in-Egypt-hit-33M-in-April-2017

'ICT and E-Commerce-An Opportunity for Developing Countries' (2003) United Nations Conference on Trade and Development. Issues In Brief No. 1

'Information Economy Report: Digitalization, Trade and Development' (2017) UNCTAD Overview accessed 15 October 2017 at http://unctad.org/en/PublicationsLibrary/ier2017_overview_en.pdf

J Althauser, 'British Treasury Plans to Implement EU-Wide Cryptocurrency Regulation by Late 2018' (December 2017) accessed at https://cointelegraph.com/news/british-treasury-plans-to-implement-eu-wide-cryptocurrency-regulation-by-late-2018

J Forder, 'The Inadequate Legislative Response to E-signatures' (2010) 26 *Computer Law and Security Review* 418

J H Abawaji, *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications* (IGI Global, 2012)

Judge E Elsonbaty, 'The Electronic Signature Law: Between Creating the Future and the Future of Creation' (2005) *Digital Evidence and Electronic Signature Law Review* www.deaeslr.org

J Kollewe, 'Bitcoin: UK and EU Plan Crackdown Amid Crime and Tax Evasion Fears' (December 2017) The Guardian accessed 7 January 2018 at https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity ; https://cointelegraph.com/news/british-treasury-plans-to-implement-eu-wide-cryptocurrency-regulation-by-late-2018

Jo Swinson (then Consumer Minister) 'Biggest overhaul of consumer rights in a generation' Press Release 27 March 2015.

K McConnell, 'Best Practices for Bitcoins: Regulatory, Legal and Financial Approaches to Virtual Currencies in Hesitant, Global Environment' (2016) Thesis accessed 5 December 2017 at http://www.aph.gov.au/DocumentStore.ashx?id=46d34817-cdc7-42a5-97ec-e3ff59bd6634&subId=301945

K M B Islam, 'E-Commerce: Laws and Cybercrime' accessed 25 November 2017 at https://www.academia.edu/694983/E-COMMERCE_LAWS_AND_CYBER_CRIMES

K C Lauden, C G Travor, *E-Commerce: Business, Technology, Society* (Pearson/Addison Wesley, 2004)

K S Barath, V Mahalkshmi, 'Legal Issues in E-Commerce Transactions- An Indian Perspective' (2016) Vol 4 Issue 11 *International Journal on Recent and Innovation Trends in Computing and Communication* 184-191

M Brown, 'Advancing E-commerce in Egypt: Legal and Regulatory Recommendations' (2000) report submitted to the Ministers of Economy and Foreign Trade and Communication and Information Technology

M Ethan Katsh, *The Electronic Media and the Transformation of Law* (University of Massachusetts Press, Boston, 1989), 22.

M Lazar, 'E-commerce Statistics and Technology Trendsetters for 2017' (March 4, 2017), IBM official website accessed 10 September 2017 at https://www.ibm.com/developerworks/community/blogs/d27b1c65-986e-4a4f-a491-5e8eb23980be/entry/Ecommerce_Statistics_Technology_Trendsetters_for_20171?lang=en

M S Wicht, 'The Tax Implications of Bitcoin in South Africa' (2016) LLM Thesis, University of Pretoria accessed 24 December 2017 at https://repository.up.ac.za/bitstream/handle/2263/60114/Wicht_Tax_2017.pdf?sequence=1&isAllowed=y

New York Department of Financial Services 'BitLicense Regulatory Framework'. Available at http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework. htm

'National Cyber Security Strategy 2016-2021' HM Government accessed 22 February 2018 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf

O Omotubora, 'Comparative Perspectives on Cybercrime Legislation in Nigeria and the UK – A Case for Revisiting the "Hacking" Offences Under the Nigerian Cybercrime Act 2015' (2016) *EJLT* Vol 7 No 3

OECD MINISTERIAL CONFERENCE "A BORDERLESS WORLD: REALISING THE POTENTIAL OF GLOBAL ELECTRONIC COMMERCE OTTAWA, 7-9 OCTOBER 1998 OECD ACTION PLAN FOR ELECTRONIC COMMERCE SG/EC(98)9/FINAL accessed 8 October 2017 at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En

'OECD E-Government Studies: Egypt 2013' (OECD Publishing, 2013), p. 70

Official Website of Dar El Ifta http://www.dar-alifta.gov.eg/Foreign/default.aspx?LangID=2&Home=1

P Chetty, 'An Analysis of Electronic Signature Regulation in South Africa' (2013) *A research report submitted to the Faculty of Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management (in the field of ICT Policy and Regulation).*

P Giliker, 'The Consumer Rights Act 2015-A Bastion of European Consumer Rights?' (2016) *Legal Studies* Vol. 37 Issue 1, pp 78-102; As acknowledged by the government in its Explanatory Notes to the Act, at [5]

P Todd, *E-Commerce Law*, (Taylor and Francis, 2017)

R Atkinson, 'Testimony before the Committee of Ways and Means Trade Subcommittee, Hearing on 'Expanding US Digital Trade and Eliminating Barriers to Digital Exports' (2016), July 13, retrieved 15 September 2017 from http://waysandmeans.house.gov/event/hearing-expanding-u-s-digital-trade-eliminating-barriers-u-s-digitalexports/

R Bone, 'The Challenges of Law in Cyberspace-Fostering the Growth and Safety of E-Commerce' Commissioner Mozelle W. Thompson, Federal Trade Commission accessed 30 September 2017 at http://www.bu.edu/law/journals-archive/scitech/volume6/presentation.pdf

R Bollen, 'The Legal Status of Online Currencies: Are Bitcoins the Future?' (December 2013), 24(4) Journal of Banking and Finance Law and Practice 272, 277

R H Christie, *The Law of Contract in South Africa* (LexisNexis/Butterworths, 2006)

R T Nimmer, 'The Legal Landscape of E-Commerce: Redefining Contract Law in an Information Era' (2006) A paper presented at the Journal of Contract Law Conference, 'Contract and the Commercialisation of Intellectual Property', presented by the Singapore Academy of Law and Singapore Management University, September 2006

R Low, S Christensen, 'E-signatures and PKI Frameworks in Australia.' (2004) *The Digital Evidence Journal, incorporating the e-Signature Law Journal* 1(2): pp. 56-59.

Revenue and Customs Brief 9 (2014): Bitcoin and other Cryptocurrencies issued 3 March 2014 accessed 7 January 2018 at https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies

R Low, S Christensen, 'E-signatures and PKI Frameworks in Australia.' (2004) *The Digital Evidence Journal, incorporating the e-Signature Law Journal* 1(2): pp. 56-59.

S Corones, S Christensen, J Malbon, A Asher, J M Paterson, 'Comparative Analysis of Overseas Consumer Policy Frameworks' (2016) Quensland University of Technology accessed 15 February 2018 at http://consumerlaw.gov.au/files/2016/05/ACL_Comparative-analysis-overseas-consumer-policy-frameworks_Part1.pdf

S C Henderson, 'Is Auditor Participation in Developing Electronic Commerce Systems: The impact on System Success' (2002) Ph.D. Thesis, Auburn University, Australia.

S E Blythe, 'E-commerce Security in the Land of the Pharaohs: Refining Egypt's Electronic Signature Law' (2011) 21 *Ind. Int'l & Comp. L. Rev.* 181

S Haig, 'South Africa Will Begin Testing Bitcoin and Cryptoregulations' (July 2017) accessed at https://news.bitcoin.com/south-africa-will-begin-testing-bitcoin-and-cryptocurrency-regulations/

S Haig, 'South Africa to Take "Balanced Approach" to Bitcoin and Cryptocurrency Regulations' (August 2017) accessed at https://news.bitcoin.com/south-africa-to-take-balanced-approach-to-bitcoin-and-cryptocurrency-regulations/

S Tarek, 'Egypt's Bitcoin Scene Seemingly Growing Despite Looming Uncertainties' (9 December 2017) Al Ahram Online retrieved 10 December 2017 at http://english.ahram.org.eg/NewsContent/3/12/282508/Business/Economy/Egypts-Bitcoin-scene-seemingly-growing-despite-loo.aspx

South Africa, The Department of National Treasury, 2014, User Alert: Monitoring of Virtual Currencies

S Kamel & M Hussein, 'The Emergence of E-Commerce in a Developing Nation: Case of Egypt', *(2002)* 9:2 *BENCHMARKING: AN INTERNATIONAL JOURNAL 146,* 146-53

, *available at* http://www.emeraldinsight.com/Insight/viewContentItem.dojsessionid=07E05F64F61893COAFB15728FB88F6F3?contentType=Article&contentId=843047. an analysis of Egypt's communications infrastructure, see *National Profile for the Information Society in Egypt*, U.N. ECON. & Soc. COMM. FOR W. ASIA (2005), *available at* http://www.escwa.un.org /wsis/reports/docs/Egypt_2005-E.pdf

S Kamel, A Ghoneim, S Ghoneim, 'The Impact of the Role of the Government of Egypt on Electronic Commerce Development and Growth' (2004) Chapter XII, Idea Group Publications, USA accessed 19 April 2017 at https://www.academia.edu/7884704/The_Impact_of_the_Role_of_the_Government_of_Egypt_in_Electronic_Commerce_Development_and_Growth

S Mason, *Electronic Signature in Law* (Cambridge University Press, 2012)

S S Malawer, 'Global Governance of E-Commerce and Internet Trade: Recent Developments (2001) Features: International Law Section accessed 29 October 2017 at http://www.worldtradelaw.net/articles/malawerecommerce.pdf.download

T R Gebba, M R Zakaria, 'E-Government in Egypt: An Analysis of Practices and Challenges' (2015) *International Journal of Business Research and Development* Vol. 4 Issue 2, pp 11-25

'The WTO's Discussions On Electronic Commerce' (2017) Analytical Note SC/AN/TDP/2017/2 retrieved 17 September 2017 from http://www.intgovforum.org/multilingual/sites/default/files/webform/AN_TDP_2017_2_The-WTO%E2%80%99s-Discussions-on-Electronic-Commerce_EN.pdf

The OECD Action Plan for Electronic Commerce was endorsed by Ministers at the OECD Ministerial Conference, "A Borderless World: Realising the Potential of Global Electronic Commerce", held on 7-9 October 1998 in Ottawa, Canada; available at http://www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)9-final.

The Guidelines for Consumer Protection in the Context of Electronic Commerce, approved on 9 December 1999 by the OECD Council, available at www.oecd.org.

The Bitcoin ETF Will Be Rejected According to Prediction Markets' accessed 20 February 2017 at https://www.cryptocoinsnews.com/the-bitcoin-etf-will-be-rejected-according-to-prediction-markets/

US Census Bureau News https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf?cm_mc_uid=80910170544715056493721&cm_mc_sid_50200000=1505649372

W Jacobs, PN Stoop, R Van Niekerk, 'Fundamental Consumer Rights under the Consumer Protection Act 2002: A Critical Overview and Analysis' (2010) *Potchefstroom Elec LJ* 303.

Z N Jobodwana, 'E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges' (2009) *Journal of International Law and Technology,* Vol. 4 Issue 4