Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (897-906)

The Risks of Electronic Piracy and its Impact on Arabic E-Commerce: Saudi Arabia as a Model

Monther Abdulkarim Ahmad Alqudah[1], &
Mohammad Hussien Mohammad Al-Ahmad[2]

Abstract

The objective of this research is to examine the legal consequences arising from attacks on electronic commerce and the associated risks. Currently, online trade is considered a fundamental pillar for major corporations, yet instances of electronic fraud and cyber piracy frequently occur during commercial transactions, particularly since e-commerce transcends geographical boundaries, making it vulnerable to cross-border cybercrimes. The researcher employed the descriptive-analytical method with a focus on legislation in the Kingdom of Saudi Arabia. The findings revealed that cyber piracy results in substantial losses for e-commerce at both the Arab and global levels, as evidenced by the cybersecurity index. The study concluded with the recommendation that Saudi Arabia should establish a specialized policy to combat cybercrimes associated with e-commerce by enforcing criminal sanctions, bolstering support for local institutions and investment bodies operating within its borders, and implementing measures and technologies to ensure the security of electronic commercial activities.

Keywords: Piracy, E-commerce, Cybercrime, Wire fraud, commercial cybercrime, cyber hacking.

Introduction

Today, e-commerce is one of the most important economic dealings between States and has been clearly influenced by modern communication techniques and electronic methods. And it has largely invested in them. The so-called electronic commerce has emerged. States and institutions dealing with the fight against cybercrime have recognized the importance of the Internet after individuals and entities have promoted their goods, or provided their services and used fake business contracts through them.

Many definitions of e-commerce can also be summarized as follows: “It is a new concept that explains the process of buying and selling or exchanging products, services and information through computer networks, including the Internet.” (Abdul Fattah, 2003, p. 17). “It is a set of integrated business operations that all actors, institutions and individuals deal with, and depend on electronic processing.” (Ra’fat, 1999, p. 33).

[1] Associate Professor of Civil Law, Faculty of Law, Amman Arab University, Amman, Jordan. Email: m.alkodah@aau.edu.jo

[2] Assistant Professor of Criminal Law, Faculty of Law, Amman Arab University, Amman, Jordan. Email: m.alahmad@aau.edu.jo

*Note: This research was published through the Scientific Research Support Fund of the Deanship of Scientific Research of Amman Arab University.

Despite this distinction of online e-commerce as a marketplace and outlet for the disposal of goods, there are crimes, risks and criminal behaviors, such as fraud, and deceit, there are no guarantees for consumer protection, as non-native, or counterfeit goods can be marketed on the Internet, with no regard to the consumer's right.

One of the most popular ways of fraudulent e-commerce is through the use of credit cards, especially when the number is known, the person who got it can buy through it. (Al-Hammouri ,2023 ,p72) In the Arab States, the first such case was seized in Egypt when two university students were able to cash half a million pounds from the balance of a government bank client through the Internet and used the amount to watch various films for seven months. This happened after finding out the secret number of the client's online account (Al-Qudah, 2020, p.50).

Cybercrime is an offence of a physical nature, consisting of any wrongful act or conduct associated with any destination or in any form with computers and computer networks, which causes the victim loss, while the offender to gain or the possibility to gain profit. These offences are often intended to steal information on computing devices, or indirectly aims at the people or entities related to such information. This type of crime has several names, including computer and Internet offences. The Saudi cybercrime regime punishes interception of any type of communication without authorization, access to accounts, credit card numbers, electronic fraud, extortion, dissemination of any content contrary to law, public order or morals, destruction of data, illegal deletion or alteration of data and electronic espionage on persons and institutions.

"There is a multiplicity of opinions on the definition of cybercrime, every opinion adopted a concept given the angle he looks through. There was one aspect of jurisprudence that defined it from a technical, and another from a legal standpoint." (Al-Qudah, 2017, p. 25).

Another aspect defines it as follows: "In view of the means or subject matter of its commission or the availability of knowledge of the information technology of the perpetrator or on the basis of other criteria as stated." (Abu Bakr, 2015, p. 60).

Literature Review

There were many views on the definition of cybercrime, every view that was conceptualized given the angle it looks through. And this led the United Nations -- its blog on cybercrime -- not to arrive at an internationally agreed definition, but was defined by the United States Technical Assessment Office by defining a computer as "Crimes in which computer data and information software play a major role". It is "a group of legally punishable acts and activities that link the criminal act to the technological revolution." It is also defined as: "Criminal activity constitutes an assault on computer software (Hijazi, 2006, p. 6).

There are also those who have defined it as: "The crime that is committed if someone uses their computer knowledge as an illegal act" (Rayan, 2002, p. 3). Article 2 of the Saudi Law on Combating Cybercrime No. 17/1428 of 16/2/2008

defines it as: Any act which involves the use of computer or information network is contrary to the provisions of this law.

Article 5 of the Saudi Law on Combating Cybercrime stipulates that: A term of up to four years' imprisonment and/or a fine of up to three million riyals shall be imposed: 1. Any person who commits any of the following information offences: unlawful entry to cancel, delete, destroy, divert, destroy, alter or reproduce private data. 2. Stopping, disabling, or destroying the information network. Scanning, deleting, leaking, destroying or modifying existing software or data. 3. Impede, disrupt or hinder access to the Service by any means whatsoever.

"Electronic commerce is a risk that may be exploited by criminals in committing their crimes. Online commerce does not have modern and sophisticated evidence that fits the new methods of this type of commerce based on the electronic communication network and modern information technologies. The lack of signed paper documents creates the problem of inability to distinguish between original message and the copy." (Abu Al-Khail, 2005, p.279).

"The magnitude of the losses caused by the phenomenon of piracy is not limited to the direct effects on the economy but has affected the migration of Arab minds expert in the software industry to the countries that safeguard intellectual property rights as a result of feeling the absence of intellectual property protection law in Arab countries." (Al-Qudah, 2020, p. 56)

The phenomenon of piracy and penetration began with the onset of the electronic calculator, and increased dramatically with the use of network technology. "It is a hack into computers often through the Internet. Because most of the world's computers are connected through this network, or even through internal networks with more than one computer." (Mohammad, n. d., p. 33)

The Saudi Law on Combating Cybercrime No. 17/1428 stipulates in article 4 that a term of up to three years' imprisonment and/or a fine of up to 2 million riyals shall be punished; Any person who commits any of the following informational offences: 1. To seize, sign, fraudulently, take a false name, or impersonate for himself or for others on a transferred money or bond. 2. Access - without valid systemic justification - to bank, credit or securities ownership data to obtain data, information, funds or services.

"An international report revealed that Saudi Arabia is the most targeted country in the Middle East, Turkey and Africa with cyber threats to the security of companies and government bodies in the region. The report produced by one of the companies specializing in the fight against cyberpiracy clarified that Saudi Arabia topped the list from among five countries in the number of advanced cyber-hacking attacks at 30 percent of the total number of recorded attacks in the first half of 2021 followed directly by Turkey at 29.5 percent. Qatar is 16 percent; the UAE is 7.1 percent and the fifth: Kuwait is 6.4 percent.

The report also noted that it was based on data collected through a cloud (FireEye Dynamic Threat Intelligence). An increase in the flow of malware in April, which may be the result of an online hacking crime campaign, or the spread of fraud

on public websites that month." (Fire Eye Electronic, Trend Micro companies, 2014)

Objectives of the Study

The problems of this study are due to a statement of roles related to commercial e-piracy crimes such as cybercrime, corporate data manipulation and its impact on e-commerce in Arab countries, and in Saudi Arabia.

This study dealt with many of the objectives, the most important of which are:

1. Contribute to providing opportunities for attention to anti-piracy institutions and agencies in Arab States and in Saudi Arabia in particular.
2. This study, which will be as comprehensive as possible to all aspects and effects of cyber hacking crimes on the e-commerce market of an Arab model, Saudi Arabia.
3. Provide new additions through reports from scientific institutions on the growth of "e-piracy" and ways to overcome it.

Research Method

First: the methodology used in the study

To this end, the two researchers will use the following methods of scientific research in their study:

1. The analytical method: through work on information collection, analysis and disaggregation.
2. The deductive method: deducting views and discussing them with a scientific methodology.
3. The descriptive method: describing the institutions and entities responsible for fighting against cybercrime.

Results and discussion

E-Commerce: "A kind of sales and purchases between producers and consumers, or between business institutions, through the use of ICT (information and communication technology)." (Al-Obaidi, Al-Ma'mouri, 2011, p. 55).and E-Piracy definition: Cyber hacking takes many forms, such as copying other people's software for use or sale, hacking networks, destroying their systems out of retaliation or embezzlement, such as entering banks' and large companies' networks without a permit, copying, modifying or deleting their databases, thereby causing them enormous losses (Hameedah, 2013, p:12).

The low contribution of Arab e-commerce globally is due to many factors, mainly to the fact that sites using Arabic do not represent more than o.5% of the Internet's use space. This is a major obstacle to the success of e-shopping in the Arab countries. The language problem is an important factor restricting the activity of Arab electronic commerce. Lack of awareness of the means of electronic commerce, namely means of meeting the price through cash payment techniques,

credit cards and weak confidence in the security aspects of information protection, were crucial factors in the poor use of this evolving pattern of business activities.

Studies suggest that crime is rising with unemployment and vice-versa. Low wages and income fluctuations are influencing criminal behavior such as selling prohibited goods, bribery and theft, all in order to achieve additional payment. And that when wages rise money-related offences decrease. The sociopolitical theory of the crime phenomenon was that it was committing an assault on money happens more in the winter; because it is due to the individual's need for food and clothing due to low income. "Yemen is ranked eighth in the world in computer software piracy and first in Arabic with 89%, followed by Libya with 87%. The least vulnerable countries to computer software hacking are the United States, Japan, New Zealand and Luxembourg, at around 20%." (Al-Ateef, 1966, p.50).

"Given the losses caused to the economies of some Arab States as a result of software piracy, many Arab States have begun to fight piracy and protect intellectual property rights, with a view to encouraging investments in the software industry and reducing losses resulting from piracy, including Egypt, Saudi Arabia, the UAE and Yemen." (IDC institute, 2003, p.4)

E-commerce has become widespread in Saudi Arabia due to the increase in per capita GDP, the development of internet networks, and the availability of numerous electronic payment methods. Electronic payments have contributed to increased flexibility in the e-commerce market, attracting a large audience to engage in online shopping and purchases. Payments are made through smart devices and e-wallets, and bank cards such as MasterCard and Visa allow for electronic payment transactions.

The Kingdom of Saudi Arabia has placed significant emphasis on investing in e-commerce and has established the E-Commerce Council. This council has imposed several conditions on e-commerce, including the requirement for electronic stores to verify their data and to clearly display their policies, terms, and conditions. Additionally, it mandates the protection of customer data and grants customers the right to return goods after purchase.

Customer data protection requires that data not be used without the customer's consent and prohibits the retention of such data for more than 14 days. Furthermore, online advertisements must be regulated to include product information, the brand name, and to prohibit the use of any third-party trademark without the owner's permission. Contact information must also be provided.

It should be noted that e-commerce in Saudi Arabia faces several challenges, such as global competition and a lack of consumer trust, as many consumers fear fraud, theft, data breaches, or the hacking of their accounts.

Electronic commerce has many characteristics that distinguish it from traditional commerce, those are:

1. The absence of a specific geographical location where sellers and buyers meet.
2. E-commerce is carried out with the highest degree of competence, most efficiently and at the lowest financial cost possible, as it relies on Electronic Data

Interchange (EDT) and documents such as sending money transfers, laws, bills of exchange and other information systems. (Hussein, 2012, p. 45)

3. Electronic commerce helps to carry out many transactions and deals easily and conveniently without requiring the seller or buyer to move where such products and services are offered.

The Kaspersky Cyber Security Index currently includes three main indicators:

- Indifferent users - indicator of users who believe they cannot become targets of cyberattacks
- Unprotected users - indicator of users who have not installed a security solution on computers, tablets and smartphones
- Affected users - Indicator of the percentage of users who have fallen victim to cyberattacks. The list of cases included in this indicator was increased in the second half of 2016.

Saudi Arabia's indicator for the second half of the year (for indifferent users, unprotected users and affected users) 44-52-79, this means that 79% of users in Saudi Arabia believe they cannot become targets of online attacks. And 52% of those who participated in the survey did not use protective solutions on all devices used in their Internet connection. And 44% of those surveyed have been subjected to cyberattacks in the last few months. The previous indicator had been 47-42-21, meaning that more people had now decided to use security measures compared to the number of such people six months earlier." (Cyber security Index. 2022, p.15)

"The Government of the Kingdom of Saudi Arabia attaches great importance to the transformation of e-government transactions, as the concepts of e-government transactions offer great benefits to the national economy. The Decree No. 7/B/33181 was issued on 10/7/1424 A.H. which includes the development of a plan for the provision of e-government services and transactions by the Ministry of Communications and Information Technology." (National Portal: Saudi Government Electronic Transactions).

"Saudi Arabia's ranking of cybersecurity threats improved during 2023, ranking 35th from 42nd in 2022. This shift indicates a globally low proportion of security threats based on sources, including malware, spam, phishing attacks, attacks on websites and networks, and independent software that has been detected from the country." (Security and Protection Company Semantec 2022). "The Ministry of Commerce and the National Consumer Protection Association of Saudi Arabia also raise awareness and warn consumers of the risks of electronic commercial fraud." (Abdul Malik, 2014, p.70).

The Kingdom of Saudi Arabia has prioritized cybersecurity and the fight against cybercrimes. In 2017, the National Cybersecurity Authority was established with the objective of developing effective strategies to protect the Kingdom's digital infrastructure and safeguard critical information. On a societal level, the Authority seeks to raise awareness of the risks posed by cyberattacks, specifically addressing electronic financial fraud and piracy targeting institutions and individuals, which

aim to steal sensitive and financial data, thus posing a threat to the nation's economic security.

In response, the Kingdom strives to counter cyber piracy and electronic fraud, as well as to protect against hacking attempts aimed at large corporations and institutions to steal customer data, access their bank accounts, and compromise their passwords. The Authority has also enhanced international cooperation in the field of cybersecurity through a number of agreements, alongside advancing national capacities and fostering cybersecurity education and training for employees.

Given the rapid development in technology and the internet globally, it is imperative for websites to adopt secure e-commerce platforms, even if this entails significant financial costs. Moreover, it is advised that e-commerce platforms utilize Secure Socket Layer (SSL) protocols to ensure that they are not exposed to hackers. Businesses are also advised not to store sensitive user data post-purchase, enforce the use of strong passwords, implement alert systems to monitor suspicious activities related to fraud and cyber piracy, utilize tracking numbers for all orders, and verify user identities, addresses, and shipment routes to bolster customer confidence.

It is further recommended that companies maintain backup copies of their electronic databases. In line with this, the National Cybersecurity Guidance Center has issued guidelines to safeguard e-commerce platforms. The Anti-Cybercrime Law also prescribes a penalty of up to three years' imprisonment and a fine of SAR 2 million for attempts to infringe upon individuals' privacy, use of aliases, or electronic theft of funds from accounts.

Conclusion

At the end of this scientific study, we must arrive at a conclusion through its parts of the findings and recommendations to reach the desired benefits of this study. Perhaps the conclusions and recommendations we present lighten the way for future researchers. First, e-commerce is a contemporary development that requires criminal protection against cybercrime in general, and against commercial fraud in particular. Second, dealing with e-commerce sites spread in the virtual world (Internet) of businesses that are now indispensable to individuals and communities in particular. Third, ways and means of combating cybercrime in relation to electronic commerce remain unclear in most Arab States for the difficulty of pursuing them and the plurality of perpetrators. Furthermore, there are legal deficiencies in laws and regulations of combating cybercrime and electronic commercial fraud in many Arab countries, and these laws in Saudi Arabia still need to be thoroughly reviewed. Also, the scale of e-commerce in Saudi society is one of the fundamental pillars of building an economically strong nation. Thus, the Saudi Law on Combating Cybercrime No. 17/1428 guarantees deterrent penalties in Articles 4-5 in order to protect individuals, business institutions and other electronic fraud or access to people's accounts without permission, or manipulation of electronic payment methods.

Recommendations

1. The Saudi State should adopt the idea of establishing an Arab security union through Arab ministers of interior affairs to combat cybercrime.
2. The State of Saudi Arabia shall provide further support to private institutions, bodies and private centers within its territory that are engaged in combating cybercrime physically and morally.
3. The Saudi State must create a special policy on combating cybercrime at both the private and official levels of the State.
4. Work on a review in order to add legal articles explicitly stipulating the protection of electronic business operations in addition to increasing punishment for offenders who repeat the offence, or those who engage in crime through gangs. Or if the electronic crime is transnational.
5. The Saudi State shall constantly and continuously organize the work of combating cybercrime.
6. Urge government departments, agencies and relevant private businesses to encourage their employees to participate in cybercrime combating courses.
7. Allowing parallel national institutions and special bodies to combat cybercrime, as well as State institutions.
8. Encouraging businesses and their employees by the State of Saudi Arabia, and providing certificates of expertise to those working in combating cybercrime.
9. Increase penalties for all contributors to attacks on electronic business operations so that all participants, whether active, instigating or interfering to achieve public and private deterrence, are punished equally.
10. Develop procedures and techniques to ensure public safety from public hazards resulting from irresponsible freedom to engage in electronic business.

References

Abu Al-Futouh, Ahmad. (2015). *Basics of electronic commerce*. Egypt: Arabic Office for Knowledge

Abu Al-Khail, Abdul Wahab. (2005). *Study on Cybercrime*. 1st edition. Saudi Arabia: Ghraib House for Printing, Publishing and Distribution

Al-Labban, Shareef. (2000). *Recent global trends in the use of electronic means*. Egypt: Egyptian Journal of Media Research

Bassiouni, Abdul Hamid. (2003). *E-commerce*. 1st edition. Cairo: Scientific Books House for Publishing and Distribution

Hussein, Osama. (2011). *Electronic Fraud (causes and solutions).* 1st edition. Saudi Arabia: Janadriyah for Publishing and Distribution

Hijazi, Abdul Fattah. (2002). *Legal System of Electronic Commerce 1st* edition. Alexandria. Dar Al-Fikir Al-Jmi'ee

Hijazi, Abdul Fattah. (2006). *Criminal Evidence and Forgery in Computer and cybercrime* .1st edition. Egypt: Legal Books House

Khaled Abdul Rahman Mohammad Khalid. (2010). *Electronic hacking and its impact on the software industry*. Egypt. : Dar Al-Fikir Al-Arabi

Ridwan, Ra'fat (1999). *The world of electronic commerce*. Arab Organization for Administrative Development. Cairo, Egypt

Rayan, Mohammad. (2002). *Computer crimes and data security*. Legal Journal .Beirut

Salim 0Mohammad Ogley. (d. t). *Investigation of computer and Internet crimes.* Legal Journal. Libya

Salamh, Ma'moun. (1979). *Penal Code General Section*. Egypt: Dar Al-Fikir Al-Arabi

Al-Atif, Jamal. (1966). *The idea of economic crime*. First Arab Social Defense Seminar. Cairo

Al-Obaidi, Ali, Al-Ma'mouri, Jasim. (2011*). The Impact of the Use of Electronic Commerce in Reducing Marketing Costs- Applied Study at Zain Telecommunications*, Faculty of Management and Economics published in the Journal of Babylon University - Humanities - 19 (issue)

Abdul Mohsen, Mohammad. (2004). *Marketing and e-commerce challenges*. Cairo: Academic Library

Abdul Rahman, Ismail (2009). *Gulf states are moving towards a unified e-commerce law*. Kuwait

Al-Arian, Mohammad. (2004). *Information crimes. Alexandria*. New University Publishing House

Abdul Hadi, Abdul Hafeez (2000). *Proposed framework for tax adjustments for the transition to the world of e-commerce - theoretical and field study*. Iraq: Journal of the University of Babylon

Kayid, Osama. (2007). *Criminal protection of private life and information banks*. Cairo: Dar Al-Nahdah Al-Arabyah

Qashqush, Huda. (1992). *Cybercrime in comparative legislation*. 1st edition. Cairo: Dar Al-Nahdah Al-ArabyahAl-Qudah, Munthir. (2020*). E-commerce legislation*.1st edition. Jordan: Wael Publishing House

Al-Qudah, Munthir. (2017*). E-Commerce Law - Saudi regulations for e-commerce*. 1st edition. UAE: International Publishing House

Al-Qudah, Munthir. (2017). *E-commerce (from a technical, economic and administrative perspective*). 1st edition. Saudi Arabia: Al-Rushd Library

Kareem, Hussein. (2012*). Arab E-Commerce... Prospects and Challenges, Qadisiyah University* - Faculty of Administration and Economics – Iraq

Kareem Hamidah. (2013). *Electronic piracy*. Egypt: Al-Alukah Net

Murad, Abdul Fattah (2003). *Use of e-commerce to sell and buy online*. 1st edition. Oman: Wa'el Printing & Publishing House

Al Mawafi, Abdul Latif. (2014). *Explanation of the UAE Information Technology Crime Law*. 1st edition. Dubai: Dubai Judicial Institute.

Al-Matradi, Muftah. (2017). *Cybercrime and overcoming its challenges.* Cairo: Sharia College Magazine - Tanta

Al-Matradi, Muftah. (2012). *Cybercrime in Gulf society and how to confront it. Adviser to the Libyan Supreme Court* - Third Conference of Presidents of the Supreme Courts of the Arab States of the Republic of Sudan, 23-25 September 2012

Najjar, Ahmad. (2002). *The problematic tax dimension in e-commerce*. Kuwait: University of Kuwait

Hilali Abdullah. (2007). *Budapest Convention against Cybercrime*. 1st edition. Cairo: Dar Al-Nahdah Al-Arabyah