COVID-19 AND E-COMMERCE THREATS IN SAUDI ARABIA

Zubeida Abdul Hadi Ateem, Prince Sultan University

ABSTRACT

The increase in the threats of electronic commerce globally is one of the effects of the Covid-19 pandemic on the economic and commercial aspects, which must be combated with strong laws and legislation, E- commerce in the Kingdom has witnessed a tremendous expansion in recent years due to the interest of Vision 2030 in it, Where the Saudi legislator issued legislation regulating Internet crimes with strict penalties for such crimes, The study aimed to identify the legal rules to combat e-commerce threats in the Kingdom of Saudi Arabia during the period of the Corona virus pandemic. By analyzing and interpreting it, by following the comparative descriptive analytical method و where the results of the study indicated the existence of legal rules that combat the threats of electronic commerce represented by malicious viruses and other crimes related to the Internet in the Kingdom of Saudi Arabia with strict penalties in the face of perpetrators. Among the most important recommendations is the necessity of having international agreements regulating these crimes and enhancing international cooperation to combat e-commerce threats.

Keywords: COVID-19, E-Commerce Threats, Saudi Arabia.

INTRODUCTION

The vision of the Kingdom of Saudi Arabia 2030 aimed at digital transformation, regulating electronic commerce, developing the infrastructure of the Internet, and issuing supporting legislation for that, Where the Council of Ministers of the Kingdom of Saudi Arabia approved the Cyber and Information Crime Control Law, which aims to limit the spread of information crimes via the Internet, and punish Internet hackers to protect individuals and institutions. According to its second article, this system aims to reduce the incidence of information crimes, by identifying these crimes and the penalties prescribed for each of them for the following:

1. Helping to achieve information security.
2. Preserving the rights resulting from the legitimate use of computers and information networks.
3. Protecting the public interest, morals, and public morals.
4. Protection of the national economy.

According to Vision 2030, the E-Commerce Council was established in the Kingdom of Saudi Arabia on 2019, the council undertakes the tasks of proposing e-commerce policies and legislation, supervising the *"electronic commerce stimulus"* program, coordinating with the relevant authorities to prevent duplication, and removing all difficulties facing e-commerce in the Kingdom of Saudi Arabia. One of the council's most important achievements in 2019 is the preparation of cybersecurity guidelines in E-commerce 2020. In addition to the issuance of the electronic commerce system 2019, this was issued by Royal Decree No. M/126, which allows

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

online buying and selling of goods, services, information, sales support and customer service (Malibari et al., 2020; Matbouli & Gao, 2012; Al-Otaibi, 2009). The Saudi Electronic Commerce Law consists of 26 articles. This law supports trust in e-commerce in the Kingdom of Saudi Arabia and encourages dealing with it and developing electronic stores, While providing the necessary protection for consumers from counterfeiting, forgery, fraud and fraud, and preserving all rights of the parties involved in electronic commerce, Especially the electronic consumer, who obtains a number of benefits by using the Internet to buy from - saving time and effort as electronic markets are opened permanently. In addition, the electronic market contains a number of commercial companies that sell goods at reduced prices; allowing small companies to compete with companies the big (Obeidat, 2009; AlGhamdi et al., 2011; Alqahtani et al., 2012). These efforts had an impact on me. Increasing the number of Internet users in Saudi Arabia to 31 million users, according to the statistics of Statista, in 2020, which caused the rapid growth of e-commerce markets in Saudi Arabia, supported by the remarkable shift from traditional shopping to online shopping and smart phone devices (DRC Report, 2020; Ezzi, 2016).

RESEARCH LITERATURE

The research article is characterized by the novelty of the topic and the scarcity of books that dealt with the impact of the pandemic on e-commerce threats in the Kingdom of Saudi Arabia, With the presence of Saudi studies and reports that discussed the impact of the pandemic on the business sector, including: The report of the DRC company in cooperation with the Electronic Commerce and Retail Association entitled (The Impact of the Covid-19 pandemic on consumer purchasing behavior in the Kingdom of Saudi Arabia - May 2020). The conclusion of the report is that electronic commerce in the Saudi market has risen significantly during the pandemic period, and the report did not address the threats to trade such as viruses or crimes. There is also another report issued by the Economic Unit of the Council of Saudi Chambers entitled (Covid 19 pandemic and the Saudi private sector) challenges and opportunities, which dealt with the impact of the pandemic on the private sector, and stressed the need to invest in the technology sector and encourage the launch of e-marketing platforms. These reports did not review e-commerce crimes, which are considered threats, so the importance of our research article is that it focused on the legal system of e-commerce threats and the repercussions of Covid 19 on them (Salem & Nor, 2020).

METHODOLOGY

The researcher used the comparative analytical descriptive approach, as it is descriptive because it is based on a thorough review of the legal rules related to the subject of the research. Based on the analysis and classification of e-commerce threats, and the identification of the various penalties that were set for these crimes during the COVID-19 pandemic. In order to reach reliable results, and on this basis, it was relied on various sources such as laws, orders and decisions, in addition to other relevant literature.

Research Questions

The importance of this study lies in its review of the legal system for protection from e-commerce threats in the Kingdom of Saudi Arabia, This study will attempt to answer the following questions:

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

1. Is there a criminalization of e-commerce threats in Saudi Arabia?
2. What are the measures taken in the Kingdom of Saudi Arabia to protect the consumer from the threats of electronic commerce during the pandemic period?
3. Is there an agreement to which the Kingdom is a party regulating the transnational e- commerce crime?

RESULTS AND DISCUSSION

Legal and Technical Concept of Electronic Commerce

Electronic commerce is the use of electronic means and modern means of communication in the completion of the exchange of goods, as for electronic business, it is the use of the Internet in the management of financial and administrative business. E-commerce is a form of electronic business (Bin Said, 2009; Thakur et al., 2016). It was defined as the electronic market in which sellers (suppliers, companies or stores) communicate with intermediaries and buyers, so that products and services are provided digitally and paid for by electronic money (Al-Masry, 2012).

The Saudi legislator defined it in Article 1 of the 2019 E-Commerce Law as *"an activity of an economic nature undertaken by the service provider and the consumer, in whole or in part, by electronic means, in order to sell products, provide services, advertise them, or exchange their data."*

The positive impact of COVID-19 on E-commerce in Saudi Arabia

In late 2019, the world witnessed the outbreak of the new Corona virus, which caused the World Health Organization to declare that it had reached the level of a global epidemic. Because of its health repercussions, the World Health Organization called. Governments to take urgent steps to stop the spread of Covid-19, which caused the general closures of all countries of the world and major cities. The effects of which extended to all aspects of life from the economy and education with the cessation of all commercial activities, which led to a scramble for relevant international organizations to find solutions to the economy and trade and to save companies and institutions from bankruptcy.

With consumers heading to electronic markets, which supports that the pandemic has a significant impact on the recovery of electronic markets, and there is a study by UNCTAD that showed that the Covid-19 pandemic has an impact on the shift of buyers to online shopping, which is considered the largest event in emerging economies *"The COVID-19 pandemic has accelerated the transition towards a more digital world"* (UNCTAD study, 2020), added, Secretary-General of UNCTAD.

As for the Kingdom of Saudi Arabia, it issued a general closure and curfew in March 2020, *"compulsory wearing a muzzle"*, social distancing, and a report obligating remote work with the development of guidelines and circulars for managing the repercussions of the Covid-19 pandemic. The Kingdom of Saudi Arabia has taken a number of decisions and legal circulars to mitigate the effects of the pandemic on the Saudi economy (Saudi Chambers of Commerce Report, 2020), Which caused the increase in electronic commerce transactions, as citizens and residents turned to the electronic information network to communicate with commercial companies and electronic stores as a gateway to accessing many goods and basic needs of the consumer and basic services such as electronic health platforms, digital cash transfers, and electronic payment systems, the Saudi Communications and Information Technology Commission presented a report showing a significant increase in data consumption during the Corona pandemic period, reaching more than 3 times the global average, after the average per capita consumption in the Kingdom

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

reached 920 MB.

The Negative Impact of Covid-19 on E-Commerce in Saudi Arabia: Covid-19 and E-Commerce Threats

The general closure due to the Covid-19 pandemic has encouraged many criminals and hackers to attack the Internet because it is difficult to arrest or discover them. These threats can be divided into two parts: malware threats, and other threats (internet crimes):

First: Among the most prominent threats to electronic commerce: the electronic virus, which means different types of malicious software. These programs may be available on the web. Viruses lead to major economic losses that extend to the loss of electronic commerce workers, and modern companies have tended to produce modern technologies to combat that (Azmi, 2009).

The International Interpol dealt with cyber-attacks related to the Covid-19 virus, and the report of the United Nations Office on Drugs and Crime for the Middle East and North Africa on Covid-19 and the Analysis of Cyber Threats (May, 2020) identified those threats represented in the following (INTERPOL, n.d.):

1. Malicious Domains: There are a large number of domains registered on the Internet whose names include the terms *"coronavirus" "corona-virus", "covid-19",* and *"covid-19".* They create thousands of new websites daily to campaign through spam, phishing or spreading malware.
2. Malware Cybercriminals are exploiting large-scale global communications related to the coronavirus to conceal their activities.
3. Ransomware: Ransomware can infiltrate systems via email messages containing contaminated links or attachments,

The Kingdom of Saudi Arabia woke up at an early stage before the pandemic crisis. Because of the seriousness of these viral threats to electronic transactions. A royal decree was issued on 2018 AD to establish the National Cyber Security Authority, which prepared the national strategy for cyber security in 2020. One of its first objectives was to manage and detect risks, develop plans, policies and standards to address them, and monitor and follow up mechanisms, while raising the level of community awareness through media awareness campaigns about the risks and threats of viruses and hackers. It also established partnerships and cooperation by sharing information related to risks (Document Regulatory Framework for Cyber Security, 2020). As stated in Article 5 of the Law on Combating Information Crimes 2008, he shall be punished by imprisonment for a period not exceeding four years and a fine not exceeding three million riyals, or by one of these two penalties; Every person who commits any of the following information crimes: suspending or disabling the information network, destroying, deleting, deleting, leaking, destroying or modifying programs or data that are present or used therein Impede interfere with, or disable access to the Service, by any means).

The interest of the Saudi legislator in combating these threats was reflected in reducing the risks of viral threats to electronic commerce in the Kingdom of Saudi Arabia during the pandemic period. There is no doubt that the legal protection of electronic commerce from hacker attacks on the electronic network would encourage investors to invest in it, as well as encourage consumers to trust electronic transactions, which would achieve the 2030 vision.

Second: Electronic commerce crimes and the penalties prescribed for them in Saudi law: Electronic commerce crimes are a type of information crime, which is the use of computer programs and systems to capture data and information processed electronically. And tampering

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

with the computer systems that contain them, for illegal purposes represented in theft and fraud (Abdullah, 2006) and trademark fraud, The Saudi Cybercrime Law (2008 AD) defines Internet crimes in its first article as: Any act committed involving the use of a computer or information network in violation of the provisions of this system. It was also defined as: an act that causes serious harm to individuals or commercial companies, in order to achieve material gains or serve political goals by using computers and modern means of communication such as the Internet (Azmi, 2009). The Saudi legislator mentioned in the 2008 Anti-Cybercrime Law a number of information crimes while specifying the penalties for them. He did not distinguish between electronic commerce crimes and other Internet crimes, which are represented in:)First - Circulation of data related to electronic commerce, such as dealing without a license, a crime of violating confidentiality and privacy of data, and a crime of deliberately declaring false data. In accordance with Article 3 of the Saudi Information Crimes Law, shall be punished by imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand riyals, or by one of these two penalties; Every person who commits any of the following information crimes:

1. Eavesdropping on what is sent through the information network or a computer - without a valid legal justification - or picking it up or intercepting it.
2. Unlawful access to a website, or access to a website to change damage or modify the designs of this website;

Second - Crimes related to the content of the electronic commerce process represented in the crimes of assaulting the electronic signature, the crime of exploiting the weakness or ignorance of the consumer in electronic sales, and the crime of tax smuggling (Hiba, 2007) Or fraud by entering, modifying, deleting or disabling information (Alsary, 2016). Theft or hacking of bank and credit accounts

(According to Article 4 he shall be punished by imprisonment for a period not exceeding three years and a fine not exceeding two million riyals, or by one of these two penalties; Every person who commits any of the following information crimes:

1. That he or someone else seize movable money or a deed, or sign this deed, by fraud, taking a false name, or impersonating an incorrect capacity.
2. Accessing - without a valid legal justification - to bank or credit data, or data related to the ownership of securities in order to obtain data, information, money, or the services it provides.

Third: Hacking e-commerce websites and deleting or disabling their data, in accordance with Article (1/5) of the 2008 Anti-Information Crimes Law; shall be punished with imprisonment for a period not exceeding four years and a fine not exceeding three million riyals, or by one of these two penalties; Any person who illegally accesses, deletes, destroys, leaks, destroys, alters or republishes private data.

Administrative Measures

It is by activating the means of securing electronic commerce by establishing specialized encryption to transfer data and information transmitted between two devices over the Internet in a secure manner so that no one can read it other than the sender or receiver (Al-Sunbati, 2008). The General Assembly of the United Nations decided a set of guidelines for organizing personal data files prepared on the computer, which were adopted in December 1990 and obligated national legislation to include them within its internal legislation, including what was stated in

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

Article (7), which stipulates that *"appropriate measures should be taken to protect files, whether against natural hazards."* Such as accidental loss or damage, or human risks such as accessing it without permission or using data in unsafe forms.

The Saudi National Cyber Security Authority, which was established in 2018, has contributed to combating electronic commerce crimes during the pandemic period, because it has prepared a guide for cyber security in electronic commerce. In addition to providing guidance to merchants using e-commerce to enhance cyber security and protect the electronic medium used, and the associated data and services, from cyber risks and threats. Providing instructions to e-commerce customers to protect them from falling victim to cyber-crimes and attacks in their e-commerce transactions, raising the level of cyber security awareness among e-commerce dealers (Cyber security guidelines for e-commerce consumers and the most important of these guidelines mentioned by the authority:

1. Protection of accounts and devices used in electronic commerce.
2. Protection of transactions related to electronic commerce.
3. Be careful when connecting to the Internet for the purpose of e-commerce.
4. To reduce the sharing of personal information by the consumer.

The Saudi Ministry of Commerce has also contributed to controlling electronic commerce in the Kingdom and reducing its crimes, as follows: The Department of Electronic Stores at the Ministry undertakes the task of supervising and following up on electronic sales outlets, verifying their compliance with the laws and regulations related to consumer protection, receiving communications from consumers and working to address them. The main functions of the administration are:

1. Monitoring electronic stores during the pandemic period
2. Strengthening cooperation and partnerships with electronic stores during the pandemic period
3. Receiving consumer complaints and reports electronically on the ministry's website. Call 1900, study and analyze it, and cooperate with the relevant authorities to develop solutions to treat it, or through the *"Maarouf"* platform for the stores registered in it.

Arab Regional Cooperation to Combat E-Commerce Threats

Electronic commerce crimes are considered cross-border and intercontinental crimes and among the agreements to which the Kingdom of Saudi Arabia is a party to deal with the matter

Arab Convention against Information Technology Crimes

It consists of 43 articles, where the agreement aims, according to the first article, of which: To enhance and strengthen cooperation between Arab countries in the field of combating information technology crimes, to ward off the dangers of these crimes in order to preserve the security and interests of Arab countries and the safety of their societies and individuals. Where information technology is defined in the second article as any physical or moral means or a group of interconnected or unconnected means used to store, arrange, organize, retrieve and process the orders and instructions stored therein. Therefore, the agreement applies to all cybercrimes; including crimes specialized in electronic commerce.

Scope of application: According to Article Three: The Convention applies to information technology crimes with the aim of preventing, investigating and prosecuting perpetrators, in the following:

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

1. Cases committed in more than one country
2. It was committed in a country and it was prepared, planned, directed or supervised in another country or countries.
3. It was committed in a country and an organized criminal group engaged in activities in more than one country.
4. It was committed in a country and had severe effects in another country or countries.

Therefore, the Kingdom of Saudi Arabia, during the pandemic period, may prosecute the perpetrators of electronic commerce crimes within the Arab countries that signed the agreement. The most important topics dealt with in the agreement are to identify information crimes that could harm e-commerce and are represented in: the crime of illegal access, including copying or destroying data, the crime of illegal interception and interruption of transmission or reception of data, the crime of assaulting and blocking data integrity, the crime of misuse of technology means The crime of forgery and electronic fraud, and crimes related to the violation of copyright and related rights, and the illegal use of electronic payment tools The agreement regulates judicial cooperation between the acceding states (Article 30 of the Convention) and grants the acceding states the power to exchange and extradite criminals between the states parties (Article 31 of the Convention), while obligating all state parties to exchange assistance among themselves. In investigations or procedures related to information and information technology crimes or to collect electronic evidence in crimes.

The Kingdom of Saudi Arabia has paid great attention to electronic commerce crimes since 2010, and this is evident in its accession to the Arab Convention against Information Technology Crimes 2010, To counter these risks, there are legal rules in the Kingdom of Saudi Arabia to protect against e-commerce threats in the period of the pandemic and the general closure since the announcement of the Covid-19 virus. Where the Saudi Information Crimes Law defines these crimes and sets severe penalties for them since 2008, In addition the Saudi legislator has developed a legislative guide for users of e-commerce websites that shows them ways to confront e-commerce threats during the pandemic period. With the establishment of a supervisory board, in addition to the fact that the Saudi Ministry of Commerce gave those affected by e-commerce the right during the epidemic period. To submit electronic complaints about electronic commerce crimes.

CONCLUSION

The research concluded that Covid-19 has negative effects on e-commerce as of the date of the World Health Organization's announcement of the virus, but there is no effect on e-commerce in Saudi Arabia, due to the presence of a legislative system. In addition to the existence of bodies concerned with e-commerce threats in the Kingdom of Saudi Arabia and guidelines for consumers of Internet services.

Recommendations

1. The necessity of establishing a regional police for electronic commerce crimes.
2. The necessity of linking the judicial communication networks in Saudi Arabia with the rest of the world to combat e-commerce crimes
3. The necessity of an international agreement on electronic commerce crimes
4. Separating electronic commerce crimes from other internet crimes in the Saudi organization
5. Holding regional and national conferences inside the Kingdom and workshops explaining the threats of electronic commerce during the pandemic period.

Citation Information: Ateem, Z.A.H. (2022). Covid-19 and e-commerce threats in Saudi Arabia. *Academy of Strategic Management Journal, 21*(3), 1-8.

ACKNOWLEDGMENTS

The author is grateful to the Prince Sultan University, Kingdom of Saudi Arabia for the financial support granted to cover the publication fee of this research.

REFERENCES

AlGhamdi, R., Drew, S., & Al-Ghaith, W. (2011). Factors influencing e-commerce adoption by retailers in Saudi Arabia: A qualitative analysis. *The Electronic Journal of Information Systems in Developing Countries*, *47*(1), 1-23.

Al-Masry, A.Q. (2012). *The digital court and information crime*. Library of Law and Economics, Riyadh - Saudi Arabia.

Al-Otaibi, M., & Al-Zahrani, R. (2009). Electronic commerce in the Kingdom of Saudi Arabia. *Research Paper. KSA: King Saud University*, 1-27.

Alqahtani, M.A., Al-Badi, A.H., & Mayhew, P.J. (2012). The enablers and disablers of e-commerce: Consumers' perspectives. *The Electronic Journal of Information Systems in Developing Countries*, *54*(1), 1-24.

Alsary, E. (2016). Saeed Al-Sari: The legal system for concluding the electronic contract Al- Halabi Human Rights Publications, Lebanon.

Azmi, M. (2009). Electronic business transactions. Legal Foundations and Applications Alexandria Book Center, Egypt.

Bin Said, L. (2009). The legal system for electronic commerce contracts, Arab Thought House, Alexandria, Egypt.

Ezzi, S.W. (2016). Exploring the characteristics of the e-commerce marketplace in Saudi Arabia. *International Journal of Economic Perspectives*, *10*(4), 5-20.

INTERPOL. (n.d.). Retrieved from https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

Malibari, M.A. (2020). The role of E-Commerce platforms in enhancing competitiveness "an exploratory study on SME's in Saudi Arabia". *Egyptian Computer Science Journal*, *44*(1).

Matbouli, H., & Gao, Q. (2012). An overview on web security threats and impact to e-commerce success. In *2012 International Conference on Information Technology and e-Services* (pp. 1-6). IEEE.

Obeidat, L. (2009). *Evidence of the electronic editor*. House of Culture for Publishing Distribution, Amman, Jordan.

Salem, M.A., & Nor, K.M. (2020). The effect of COVID-19 on consumer behaviour in Saudi Arabia: Switching from brick and mortar stores to E-Commerce. *International Journal of Scientific & Technology Research*, *9*(07), 15-28.

Thakur, K., Ali, M.L., Gai, K., & Qiu, M. (2016). Information security policy for e-commerce in Saudi Arabia. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 187-190). IEEE.

UNCTAD Study. (2020). The Association of E-Commerce and in cooperation with the Brazilian Information Center Network for Digital Commerce October 2020 https://news.un.org/ar/story/2020/10/1063552

Received: 24-Nov-2021, Manuscript No. ASMJ-21-10013; **Editor assigned:** 26-Nov-2021, PreQC No. ASMJ-21-10013(PQ); **Reviewed:** 17-Dec-2021, QC No. ASMJ-21-10013; **Revised:** 14-Feb-2022, Manuscript No. ASMJ-21-10013(R); **Published:** 24-Feb-2022