LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S5(2025)

LEGAL CHALLENGES IN CONFRONTING INTERNET FRAUD CRIMES IN THE KINGDOM OF SAUDI ARABIA

Dr. Mohammed bin Fahad Ali Aljadhay[1]

[1]Vice–Dean– Collage of Law - Dar Al Uloom University.

M.aljadhay@dau.edu.sa[1]

Abstract:
This article considers the Challenges of fighting crimes on the Internet and defines Fraud Crimes acts committed by means of computer networks. The aim of the study is to develop a categorical conceptual instrument, to separate a serious type of cybercrime. The methodological basis of the analytical method by reviewing and analyzing the relevant Saudi laws issued on this matter. The conducted study allows to offer the authors' definition of Internet Fraud Crimes in the Kingdom of Saudi Arabia and their identify the distinctive features, to allocate it in an independent kind of a crime and offer to include the legal solutions.

Keywords: Fraud, Internet, cybercrime, Challenge, Hacking.

Introduction:

The continuous and evolving development of technology's role in the information society has led to an increased awareness of the importance of information as a source of power and wealth. This shift is closely linked to the global expansion of internet usage, where communication networks and information technologies have provided numerous advantages, enabling many traditional activities to be carried out more efficiently. Moreover, the internet has facilitated communication between individuals without geographical or temporal limitations. However, these advancements have also introduced limitless risks in the online world, where the network can be used illegally, resulting in a state of informational chaos across the virtual world. This has increased the prevalence of online fraud crimes, which suffer from ineffective monitoring due to the inability of criminal laws to keep pace with the rapid developments in the digital realm.

With the advancement of technology and the increased use of the internet, it has become easier for perpetrators to exploit it for committing crimes. These and other factors have contributed to the complexity of tracking online fraud crimes, as digital evidence may be weak or quickly disappear, necessitating swift action to preserve such evidence and prevent its destruction. This requires cooperation between the authorities of the country where the crime originated or the countries involved in the criminal activities. What further complicates matters is that these emerging crimes are rapidly occurring and cross-border in nature, leading to difficulties arising from differing legislations across various countries, potentially resulting in conflicts of jurisdiction regarding online fraud crimes that cross national borders, thus creating a situation of multiple and conflicting jurisdictions.

This research was founded by the General Directorate of Scientific Research & Innovation, Dar Al Uloom University, through the Scientific Publishing Funding Program.

This research was founded by the General Directorate of Scientific Research & Innovation, Dar Al Uloom University, through the Scientific Publishing Funding Program.

Importance of the Research:

With the spread of online fraud crimes, which are considered one of the biggest challenges facing society, there is an urgent need to enhance security awareness and develop effective strategies to combat this crime. This requires cooperation between governments, security agencies, and individual users to ensure a safer digital environment. Studies indicate that these crimes have a widespread impact, not only on individuals but also on all entities, leading to significant financial and material losses and a loss of trust. Furthermore, the global nature of the internet makes it difficult to track perpetrators, as they are spread across various countries. Thus, the importance of this topic becomes clear in all aspects, as it safeguards individuals from harm and preserves their property and privacy, which are guaranteed by all legal systems and ensured by the protection of all relevant laws.

Reasons for Choosing the Research Topic:

1. This research addresses an issue of great importance, especially as it affects the reputation and economy of the Kingdom.
2. The researcher feels the urgent necessity of this topic from a behavioral perspective, affecting both the individual, society, and the international entity.
3. The firm and serious stance of Islamic law towards fraud in all its forms and varying objectives.
4. The researcher's belief that online fraud activities will continue to spread and expand, leading to increasing complexity that may result in disputes at the regional and international levels.
5. The potential involvement of covert organizations that aim purely for profit and facilitate their operations to achieve their objectives.

Research Objectives:

1. To clarify the concept of online fraud crimes.
2. To highlight the reality of online fraud crimes in Saudi Arabia.
3. To identify the main challenges facing legal professionals when pursuing online fraud criminals.
4. To highlight the impact of online fraud crimes on security in the Kingdom.
5. To shed light on the most important forms of cooperation between the Kingdom and other countries involved in this issue.
6. To outline the legal penalties imposed on perpetrators of online fraud crimes in the Kingdom.

Research Terms:

- **Crime**: Any act or omission punishable by law, considered an assault on a legally protected interest, whether individual or collective (Salama, 2010).
- **Fraud**: A deceptive act committed by a person to gain an unlawful benefit (Nasirat, 2018).
- **Hacking**: Unauthorized access to computer systems, networks, or data using technological means (Hassan, 2018).
- **Internet**: All technical means used to process and exchange digital data over networks (Hassan, 2018).
- **National Security**: The ability of the state to protect its sovereignty, stability, and the safety of its land and citizens from internal and external threats (Al-Turki, 2024).

Research Problem: The lack of precise legal definitions of fraud and online fraud crimes presents a challenge for those seeking a universally agreed-upon concept, which would allow for the unification of actions that can be taken in response. The multiplicity of online fraud forms, motives, and the surrounding circumstances plays a pivotal role in classifying the crime. Therefore, the research problem concerns these crimes in detail, including their concepts, regulations, and the determination of criminal responsibility, relying on Saudi laws that address them.

Research Questions: It is clear from the title of the research that the main question is: What are the main legal challenges in pursuing online fraud crimes in the Kingdom of Saudi Arabia? This question branches into several sub-questions that also require legal and research-based answers:

1. What is the definition of fraud?
2. What are online fraud crimes?
3. What is the concept of electronic law?
4. What are the challenges facing legal professionals in combating online fraud crimes?
5. What is the impact of online fraud crimes on security in Saudi Arabia?
6. What is the reality of online fraud crimes in the Kingdom of Saudi Arabia?

Research Methodology: The research will rely on the analytical method by reviewing and analyzing the relevant Saudi laws issued on this matter.

Previous Studies:

1. **Mamdouh bin Rashid bin Mashraf Al-Anzi**. The Subjective Aspect of Fraud through Websites in Saudi Law Compared to Egyptian and Kuwaiti Law, *The Arab Journal of Security Studies*, Department of Law, College of Science and Humanities, Shaqra University, Kingdom of Saudi Arabia. 2022.
   This study indicated that fraud is a crime that represents an assault on a person's financial integrity through the use of information law, and it has increased with the growing use of websites on a daily basis and the spread of credit cards in purchasing and money transfer operations.
2. **WadiMarabitBushra, et al.** The Role of Influencers in the Spread of Fraud and Deception through Social Media Platforms, Specifically Instagram – A Field Study on a Sample of Students from the Media Department at Bouira University, Faculty of Social and Human Sciences, AkliMohandOulhadj University, Bouira, 2021-2022.
   This study concluded the necessity of focusing on the content of influencers' posts on social media first, rather than looking at their number of followers, as fame is not a measure of influence on public attitudes and behaviors. It also emphasized the need for rational use of these platforms, the legal oversight of them, and the selection of appropriate influencers to emulate positively.
3. **Samer Salman Abdel Jabouri**. Cyber Fraud Crime: A Comparative Study, College of Law, Al-Nahrain University, 2014.
   This study examined types of cybercrimes and their criminal handling by presenting computer crimes and identifying the people who commit them, as well as the history of computer intrusion in various countries. It also discussed internet crimes, including crimes against individuals and crimes related to financial fraud and e-commerce, through outlining investigation rules for cybercrimes.
4. **Shahd Mohammed Al-Shahrani**. Electronic Fraud Crime in Saudi Law, A Comparative Study, College of Law, King Abdulaziz University, 2014.

The study revealed the legislative gap in addressing electronic fraud crimes in Saudi Communications Law, Saudi Electronic Transactions Law, and the executive regulations for the securities market, compared to other jurisdictions, particularly U.S. legislation. It pointed out that the Saudi Anti-Cybercrime Law lacks comprehensiveness in fully addressing this type of crime.

Research Plan:

Introduction: (Included the importance of choosing the research, reasons for its selection, its objectives, the research problem, questions, previous studies, research methodology, and its divisions) with three chapters, conclusion, and indexes as follows:

- **Chapter One**: The Concept of Internet Crimes: It includes three topics:
  - **Topic 1**: The History of the Emergence of Internet Crimes.
  - **Topic 2**: The Concept of Internet Crime in Saudi Law.
  - **Topic 3**: The Concept of Internet Crime in Positive Laws.
- **Chapter Two**: The Reality of Internet Fraud Crimes in Saudi Arabia: It includes three topics:
  - **Topic 1**: Types of Internet Fraud Crimes.
  - **Topic 2**: The Risks of Internet Fraud Crimes to National Security.
  - **Topic 3**: How to Confront Internet Fraud Crimes.
- **Chapter Three**: Legal Challenges and Penalties for Perpetrators of Internet Fraud Crimes:
  - **Topic 1**: The Stance of Laws on Internet Fraud Crimes.
  - **Topic 2**: Methods of Protection from Internet Fraud Crimes.
  - **Topic 3**: Penalties for Internet Fraud Crimes in Saudi Law.

Conclusion: It includes two topics:

- **Topic 1**: Key Findings.
- **Topic 2**: Recommendations.

Indexes, which include:

- **Index of Sources and References.**
- **Index of Topics.**

Chapter One

The Concept of Internet Crimes

The internet has become an integral part of modern life, being used in all economic, social, and political fields, leading to a radical transformation in the ways individuals, institutions, and governments interact. With this immense development, a new set of security and legal challenges have emerged, among the most prominent of which are internet fraud crimes. These crimes have significantly increased with the rise in the use of digital technologies in daily transactions. These crimes now pose a growing threat to individuals by violating their privacy and stealing their data, to institutions through exposure to cyberattacks and financial fraud, and to national security by targeting vital infrastructure of countries.

Therefore, this chapter focuses on presenting three main topics:

- **Topic One**: The History of the Emergence of Internet Fraud Crimes
- **Topic Two**: The Concept of Internet Crime in Saudi Law
- **Topic Three**: The Concept of Internet Crime in Positive Laws

Topic One

The History of the Emergence of Internet Crimes

With the tremendous development in digital technology and the widespread use of the internet in various aspects of life, many challenges related to cybersecurity have emerged, the most prominent of which are internet crimes that gradually developed with the increasing reliance on digital networks. Internet fraud crimes were not as complex or organized in the beginning as they are today; they started with simple methods targeting individuals and institutions in a rudimentary way, and later evolved to include more complex and dangerous criminal activities. The following outlines this development:

The Early Beginnings of Internet Crimes:

The roots of internet crimes go back to the 1960s and 1970s when the use of computers began to expand, especially in government institutions and major research centers. At this stage, crimes were limited to attempts to breach computer systems to obtain information or damage data, without any financial or commercial motives as we see today. One of the earliest recorded crimes in this field was the hacking attempts that targeted the U.S. Department of Defense's communication networks during that period (Al-Maliki, 2015).

The 1980s: Expansion of Personal Computers and the Rise of Financial Crimes:

With the spread of personal computers and the emergence of new operating systems in the 1980s, the risks associated with technology usage increased, and the first instances of financial internet crimes began to appear. During this period, malicious software (viruses) emerged, used to spy on users or disrupt major companies' systems, the most prominent being the Morris Worm virus, which infected thousands of computers in 1988, highlighting the dangers of digital threats.

Second Phase: The Expansion of Internet Usage and the Emergence of Modern Crimes:

As the internet entered commercial use in the 1990s, cybercrimes began to evolve further. Phishing and financial fraud crimes via email emerged, marking the beginning of the spread of fake websites designed to steal users' data or exploit them financially. This era also witnessed the first financial hacking attempts targeting banks and financial institutions, prompting governments to consider enacting laws and regulations specifically for internet crimes. In the United States, the first law to combat cybercrimes, the "Computer Fraud and Abuse Act," was passed in 1986, marking the beginning of legal efforts to combat these crimes (Al-Maliki, 2015).

The Modern Era and the Rise of Organized Cybercrime:

With the development of the internet and the entry into the digital transformation era in the 21st century, cybercrimes became more complex and organized. Criminal networks operating online began using advanced techniques such as encryption and identity concealment, making them harder to track. Internet fraud crimes, including hacking bank accounts, identity theft, and fraud involving digital currencies, became widespread. In the last decade, the internet has become a fertile ground for new types of cybercrimes, such as fraud via mobile apps, ransomware attacks, and e-commerce fraud. This has led many countries to enhance their cyber legislation to protect national and economic security from these threats (Al-Maliki, 2015).

Conclusion:

It can be said that internet crimes have gone through various developmental stages, starting from simple hacking attempts motivated by curiosity in the 1960s, to complex organized crimes threatening institutions and countries in the modern era. As technological development

continues, these crimes are expected to increase in complexity, which necessitates the development of legal and technical frameworks capable of effectively combating them.

Topic Two

The Concept of Internet Crime in Saudi Law

Crime is a concept that changes over time, adapting to the social and technological developments occurring in the world. With the emergence of the internet, this concept has become more complex due to the proliferation of crimes committed in cyberspace. According to Saudi law, national legislation was issued to regulate the handling of these crimes. The Anti-Cyber Crime Law was introduced by Royal Decree No. M/17 on 8/3/1428H, based on Cabinet Resolution No. (79) on 7/3/1428H, providing a clear legal framework for defining these crimes and the penalties associated with them. The law defines an internet crime as: "Any act committed using a computer or an information network in violation of the law, which causes harm to individuals, institutions, or impacts public, economic, or social security." This definition encompasses a wide range of illegal actions committed online, whether they aim to commit financial fraud, violate privacy, manipulate digital information, or hack into electronic systems, making it one of the most comprehensive definitions in Arab legislation. This definition reflects the Saudi law's commitment to addressing all forms of electronic crimes that may harm individuals or society, with particular emphasis on crimes that affect national or economic security. Some argue that this definition keeps pace with rapid technological advancements, as cyberspace has become a vital environment where the internet is exploited for various criminal activities, including fraud, cyber espionage, spreading rumors, and threatening the country's information security (Abdul Razzaq, 2023).

There are various forms of internet crimes that are punishable under Saudi law, including online fraud, which is carried out through digital means to deceive victims and seize their money; privacy violations by hacking personal data or publishing sensitive information about individuals without their consent; and online defamation, which involves posting harmful content on the internet to damage the reputation of a person or entity. The law also criminalizes cyber piracy, which includes hacking digital systems, stealing information, or disrupting electronic services. Saudi Arabia has established strict legal mechanisms to combat these crimes, with the Public Prosecution investigating cases related to cybercrimes. Penalties are applied according to the Anti-Cyber Crime Law, which specifies penalties that can range from up to ten years in prison and financial fines that can reach up to five million Saudi Riyals, depending on the type and severity of the crime. Additionally, Saudi Arabia has made significant efforts to enhance cybersecurity through the National Cybersecurity Authority, which works to set policies and legislation to protect Saudi cyberspace from breaches and digital crimes.

It is clear from the above that Saudi law has adopted a comprehensive concept of internet crime, taking into account modern technological developments and providing a legal framework that defines criminal acts and their penalties, ensuring legal protection for individuals and institutions. Saudi legislation also aims to address the challenges arising from cybercrimes by providing a safe digital environment and enhancing cooperation with international bodies to track criminals and bring them to justice.

Topic Three

The Concept of Internet Crime in Positive Laws

Internet crime is defined in positive laws as: any unlawful act committed using a computer, the internet, or any digital means, aimed at harming individuals, institutions, property, or public security (Al-Badawi, 1432H). This definition includes a wide range of crimes such as online fraud, system hacking, data theft, privacy violations, spreading false information, digital piracy, and cyber extortion.

Legislation in different countries varies in its formulation of the concept of internet crime, depending on the level of digital advancement and the electronic threats they face. However, there is a convergence in the basic concepts, which include the use of the internet as a tool to commit crimes, causing harm to society or individuals, and exploiting technical vulnerabilities to gain unlawful benefits. The U.S. law defines it as: "Unauthorized use of protected computer systems or data files, or the intentional harmful use of computers or data files, with the severity of the crime ranging from a second-degree misdemeanor to a third-degree felony" (Al-Afifi, 2013, p.7).

In British law (Computer Misuse Act - CMA 1990), internet crime is defined as "the illegal use of computers or networks to achieve unlawful purposes such as electronic theft, financial fraud, digital espionage, or privacy violations." This law emphasizes the pursuit of hackers and cyber intruders who use the internet to carry out cyberattacks (Al-Thunayan, 2012, p. 8). French law (Digital Penal Code - 2004) defines internet crime as "any act committed by a person using an electronic medium to manipulate information or data, or hack digital systems in an unlawful manner, whether for theft, extortion, espionage, or disruption" (Al-Badawi, 1432H). Regarding Gulf legislation, the Gulf Cooperation Council (GCC) countries have sought to adopt strict laws to combat cybercrimes due to the direct threat they pose to the digital economy and cybersecurity.

In Kuwaiti law, Law No. 63 of 2015 on combating information technology crimes defines cybercrimes as "any unlawful use of a computer or information network that causes harm to individuals, property, or national security." The law sets penalties ranging from up to ten years in prison and large financial fines, depending on the crime and its severity.

In the United Arab Emirates, Federal Law No. 5 of 2012 on combating cybercrimes specifies the scope of digital crimes, penalizing acts such as financial fraud, cyber espionage, publishing content that threatens national security, piracy, and online defamation. Penalties in some cases can reach life imprisonment, especially if the crime aims to destabilize or threaten national security.

Qatar's law, Law No. 14 of 2014 on combating cybercrimes, defines digital crimes comprehensively, imposing strict penalties for anyone who uses the internet for unlawful purposes such as hacking systems, espionage, fraud, or publishing false news that harms individuals, institutions, or national security.

It is evident from the above that the positive laws in various countries have sought to establish comprehensive definitions of internet crimes, with some differences in the details between countries according to the nature of the electronic challenges they face and their adopted criminal policy.

Chapter Two

The Reality of Online Fraud Crimes in Saudi Arabia

The Kingdom of Saudi Arabia has witnessed rapid digital development, which has contributed to an increasing reliance on the internet across various economic, social, and administrative sectors.

However, this development has been accompanied by a rise in the rates of cybercrimes, which now threaten individuals, institutions, and national security. With the escalation of these threats, the Kingdom has placed great importance on enhancing its cybersecurity by developing legislation, adopting advanced technological mechanisms, and raising public awareness of the risks of cybercrimes and ways to combat them.

This chapter, therefore, discusses the reality of online fraud crimes in Saudi Arabia through three main sections:

- The first section discusses the types of internet crimes.
- The second section addresses the risks of these crimes and their impacts on national security.
- The third section explores how to confront online fraud crimes.

Section One

Types of Internet Crimes

With technological advancements and the widespread use of the internet in various aspects of life, cybercrimes have proliferated and now pose a significant threat to individuals, institutions, and nations. These crimes are characterized by their diversity, as they include fraudulent activities, privacy violations, and attacks targeting the digital infrastructure of countries. Although these crimes differ in their methods and objectives, they all share the use of the internet and technological means as primary tools for their execution. Below are the most prominent types of internet crimes (Abu Ghalion, 2009):

First: **Online Fraud Crimes**

Online fraud crimes are among the most common types of internet crimes. They involve the use of the internet to deceive individuals or businesses to steal money or information. These crimes include phishing, where fraudulent emails or text messages are sent to trick victims into disclosing personal or financial data. They also include fraud through fake online stores that sell non-existent products or request payment without providing any service.

Second: **Hacking (Cyber Piracy)**

These crimes involve breaching electronic systems and digital accounts to access sensitive information, whether for commercial, espionage, or sabotage purposes.

Third: **Cyber Extortion Crimes**

Cyber extortion crimes occur when perpetrators use private information or images of victims to extort money or force them to take certain actions under the threat of exposing this information. These crimes target individuals, celebrities, and businesses, and can lead to severe legal and social consequences.

Fourth: **Privacy Violations and Identity Theft**

These crimes involve stealing personal data of individuals or companies and using it for illicit purposes, such as creating fake accounts or conducting illegal transactions. This data may also be used in financial crimes, such as defrauding banks or making transactions under the victim's name without their knowledge.

Fifth: **Online Defamation and Libel Crimes**

This type of crime involves publishing false or harmful information about individuals or institutions online with the intent to damage their reputation. These crimes include defamation campaigns on social media or spreading false news to influence the image of individuals or companies.

Sixth: **Terrorist Crimes and Incitement to Violence Online**
These crimes involve using the internet to spread extremist ideas, incite violence, or recruit individuals to join terrorist groups. They also include publishing content aimed at destabilizing national security.
Seventh: **Cyber Forgery Crimes**
These crimes involve manipulating digital data, such as forging official documents, certificates, or credit cards to use them for illegal purposes. They are often carried out using specialized software to modify or create fake documents that appear genuine (Abu Ghalion, 2009).
Eighth: **Money Laundering Crimes Online**
These crimes involve using digital platforms to conceal the origins of illicit funds by transferring them through complex networks of digital transactions to hide their true source. They also include exploiting cryptocurrencies like Bitcoin to move money illegally.
Ninth: **Ransomware Extortion Crimes**
These crimes involve using malicious software to encrypt users' or businesses' data, and then demanding a ransom to decrypt it and restore access to the files. Such attacks often target financial institutions, hospitals, and government entities.
Tenth: **Crimes Related to Illegal Content**
This category includes publishing illegal content online, such as illegal pornography, drugs, weapons, or promoting legally prohibited practices. These crimes also include the spread of fake news that affects the economy or social stability (Abu Ghalion, 2009).
In relation to the Kingdom of Saudi Arabia, the Anti-Cybercrime Law identifies several types of online crimes that are considered illegal, including:

- **Online Fraud Crimes**: This includes online financial fraud and the illegal use of credit cards or banking information to achieve financial gains.
- **Unauthorized Access Crimes**: Such as hacking personal accounts or electronic systems without prior authorization.
- **Crimes Affecting National Security**: This includes publishing information that harms national security, the economy, or public law online.
- **Privacy Violations**: Such as publishing personal information about others without their consent.
- **Defamation and Cyber Extortion Crimes**: Involving threatening individuals with the publication of their private information for unlawful purposes.
- **Money Laundering Crimes Online**: Using digital channels to pass illicit funds.
- **Digital Forgery Crimes**: Such as manipulating digital official documents or forging electronic signatures.

Section Two
Risks of Online Fraud Crimes on National Security
With the rapid technological advancements and the widespread use of the internet in various life sectors, online fraud crimes have become a serious threat to national security, including in the Kingdom of Saudi Arabia. With the increasing rates of cyberattacks and online fraud, Saudi national security is facing new challenges that require advanced strategies to address. The danger of these crimes lies in their transnational nature and their ability to affect digital infrastructure, economic institutions, and social security, necessitating strengthened efforts to combat them

effectively. Below are the main risks of internet crimes to national security (Abdul Razzaq, 2023):

First: **Threat to Digital and Informational Infrastructure**

The Kingdom heavily depends on technology in vital sectors, such as energy, health, banking, and communications. Attacks on these sectors could lead to the disruption of essential services, posing a direct threat to national security (Abdul Razzaq, 2023).

Second: **Threat to Economic and Financial Security**

Cybercrimes, especially financial fraud, are among the key risks threatening economic stability in the Kingdom. These crimes affect financial institutions, businesses, and investors, leading to the loss of substantial amounts of money due to breaches and cyber fraud.

Third: **Threat to Social and Political Security**

Cybercrimes increasingly affect social fabric and political stability, including by spreading rumors and misinformation via social media, which could destabilize social order and sow discord among society's different factions. Additionally, online defamation and extortion, where individuals' personal information is exploited in smear campaigns or blackmail, threaten the social and psychological security of the community. Cybercrime also affects public opinion and manipulates political trends through misleading media campaigns aimed at targeting Saudi Arabia and tarnishing its international image.

Fourth: **Threat to National and Sovereign Security**

Certain external parties may use the internet to target Saudi national security.

Fifth: **Threat to the Privacy of Individuals and Society**

Privacy violations and identity theft are among the most prominent threats the Saudi society faces in the realm of cybercrimes, where personal accounts are hacked, and private information is stolen, leading to its use in fraud or defamation. Furthermore, surveillance of communications and data threatens citizens' privacy and exposes them to cyber extortion.

In conclusion, online fraud crimes present a significant threat to Saudi national security, with far-reaching effects on infrastructure, the economy, social, political, and sovereign security.

Section Three

How to Combat Online Fraud Crimes

With the rapid development in information and communication technologies, online fraud crimes have become an increasing threat to national, economic, and social security, requiring the adoption of comprehensive strategies to confront them. Legal regulations are fundamental in combating online fraud crimes, as they help criminalize associated actions such as cyber fraud, system hacking, data theft, and online defamation, with severe penalties for perpetrators to ensure both general and specific deterrence. In this regard, the Kingdom has issued the Anti-Cybercrime Law, which clearly defines the penalties imposed on various forms of cybercrimes and strengthens law enforcement mechanisms to combat them effectively (Anti-Cybercrime Law, 1428H).

In addition to legislation, enhancing cybersecurity is an essential necessity to protect the Kingdom's digital infrastructure from cyberattacks targeting government institutions and vital sectors such as energy, banking, and communications. This requires using advanced technologies such as encryption systems to protect data from breaches and implementing advanced mechanisms to detect intrusions and counter cyberattacks before they occur, along with enhancing cybersecurity in critical institutions to ensure continuity of services and prevent

disruptions caused by cyberattacks. To achieve these goals, the Kingdom has established the National Cybersecurity Authority, which works on setting policies and procedures to protect the national cyberspace and enhance the readiness of relevant entities to tackle electronic threats (National Cybersecurity Strategy, 2023).

Beyond technical efforts, public awareness plays a crucial role in reducing the risks of online fraud crimes, as awareness enables individuals and institutions to take preventive measures to protect their digital data. This includes training individuals on how to maintain their electronic privacy, informing them about cyber fraud tactics and phishing schemes targeting their personal and financial information, and teaching institutions how to implement strict security policies such as regular system updates and managing access permissions to sensitive data. In this context, the Kingdom has launched many awareness initiatives, including e-literacy campaigns and cybersecurity training programs, to enhance public awareness of the risks of cybercrimes and preventive measures (Al-Otaibi, 2023).

Given the transnational nature of online fraud crimes, international cooperation has become a pivotal element in combating them, as it facilitates the exchange of information about cybersecurity threats and tracking cybercriminals across borders. The Kingdom has prioritized strengthening its cooperation with countries and international organizations by joining international agreements related to combating cybercrimes, such as the Budapest Convention, and coordinating with relevant entities like Interpol to pursue cybercriminals and exchange information about emerging cyberattack methods. The Kingdom is also working to establish bilateral agreements to enhance cooperation in cybersecurity, ensuring the development of a comprehensive digital protection system capable of effectively combating cyber threats.

To develop national capabilities in cybersecurity, it has become essential to train national personnel by incorporating cybersecurity into academic curricula, organizing specialized training programs in digital forensics and cybercrimes, and encouraging research and innovation in electronic protection to develop local solutions to face digital threats. The Kingdom has launched several initiatives in this regard, including the National Cybersecurity Academy, which aims to train Saudi talents in this field, thereby strengthening the Kingdom's ability to deal with increasing cyber challenges (National Cybersecurity Strategy, 2023).

Combating online fraud crimes requires a comprehensive strategy that includes developing laws, enhancing cybersecurity, spreading awareness, intensifying international cooperation, and investing in building national capabilities. The Kingdom is committed to applying these strategies continuously through advanced organizational and technical efforts aimed at protecting the community and economy from electronic risks, solidifying its position as a leader in digital security, and ensuring a safe and sustainable digital environment that keeps pace with global technological developments.

Section three: Legal Challenges and Penalties Imposed on Perpetrators of Online Fraud Crimes

With the rapid advancement of digital technology, online fraud crimes have become one of the most widespread threats, prompting countries to adopt strict legislation to combat them. Despite the efforts made, there are still legal challenges that hinder the effective prosecution of perpetrators, especially due to the cross-border nature of these crimes. This necessitates the development of more comprehensive legal frameworks and enhanced international cooperation in this field.

This chapter is divided into three main sections:

- **Topic One**: The legal stance on the internet.
- **TopicTwo**: Methods of protection against online fraud crimes.
- **TopicThree**: Penalties for online fraud crimes in Saudi law.

TopicOne: The Legal Stance on the Internet

This section discusses the legal stance on the internet, with the first subsection focusing on the stance of European laws and the second on the stance of Arab laws and the Gulf Cooperation Council (GCC) laws.

Subsection One: The Stance of European Laws on the Internet

Several European countries have enacted specific laws to address internet and computer crimes, including the UK, Netherlands, France, Denmark, Hungary, Poland, Japan, and Canada. These Western countries have also established special departments for combating internet crimes and have taken the step of creating centers to assist victims of these crimes.

The world has witnessed many international and regional agreements aimed at combating online fraud, including the **Budapest Convention**. On April 20, 2000, the European Crime Problems Committee (CDBC) and the experts' committee in the field of technology crimes (Cyber Crime) presented a draft convention on computer crimes. The provisions of this convention were discussed and reviewed from its initial draft until its final version, which was approved in Budapest in 2001, known as the Budapest Convention 2001 (Cybercrime Convention). This agreement reflects the significant efforts of the European Union, the Council of Europe, and their expert committees focused on computer crimes and their purposes. (Al-Malki, 2015, p. 90)

Some notable international laws that have contributed to combating online fraud include:

- **Swedish Data Law of 1973**: Sweden was the first country to enact legislation against internet crimes or information crimes, particularly data forgery. The Swedish Data Law of 1973 addressed issues related to unauthorized access to computer data, data forgery, conversion, and illegal acquisition of data.
- **Danish Computer and Internet Crime Law (1985)**: In 1985, Denmark passed its first laws regarding computer and internet crimes, which included penalties for computer crimes such as data forgery.
- **UK Forgery and Counterfeiting Law (1986)**: The UK introduced the Forgery and Counterfeiting Act of 1986, which defined forgery tools, including various computer storage media and other devices used for recording data.
- **German Computer Forgery Law (1986)**: The German legislator enacted the Computer Forgery Law in 1986.
- **French Information Forgery Law (1988)**: France introduced Law No. 19 in 1988, aimed at combating information forgery.
- **Cybercrime Convention (2001)**: This convention, signed in Budapest in November 2001, was adopted by 30 countries, including the United States, which ratified it in September 2006. The convention entered into force on January 1, 2007.

Subsection Two: The Stance of Arab Laws and the Gulf Cooperation Council (GCC) on the Internet

In the Arab world, the Gulf Cooperation Council (GCC) has introduced several legal measures to combat internet fraud crimes. The GCC member states agreed on a unified law for combating cybercrimes. In the 33rd summit held in Bahrain in December 2012, the GCC decided to approve

the Unified Law for Combating Information Technology Crimes as a guiding law for a period of four years, renewable automatically unless comments are made by the member states. This law, called "The Riyadh Document for the Unified Legal System for Combating Information Technology Crimes," aims to prevent the misuse of technology and fraud.

This law is part of a series of guiding laws created to enhance judicial and legal cooperation between GCC countries. It consists of 39 articles that include types of information technology crimes and penalties for their perpetrators. The law includes severe financial penalties, with the total penalties amounting to over 11 million riyals, with variations depending on the severity of the electronic crime committed. Penalties include imprisonment for up to one year and fines of up to 500,000 riyals, or both, for individuals committing any of the crimes mentioned in the information security law. The law also covers crimes like unauthorized access to websites, altering or damaging websites, and the misuse of mobile phones equipped with cameras to harm individuals' privacy. The maximum penalty can include up to ten years in prison and fines of up to five million riyals for those involved in terrorist activities or promoting terrorism through online platforms.

Some notable Arab laws that have contributed to combating online fraud include:

- **Oman's Cybercrime Law (2001)**: Oman enacted a decree (Royal Decree No. 72/2001) to amend the Omani Penal Code to address computer crimes. Additional provisions were made under the Omani Communications Law to prevent the exchange of offensive messages and the misuse of communication devices for harassment or obtaining confidential information.
- **Moroccan Cybercrime Legislation (2003)**: Morocco introduced provisions under Law No. 07.003 of 2003, which criminalizes acts that harm automated data systems.
- **UAE Information Technology Crimes Law (2006)**: The UAE was the first Arab country to introduce a separate law to combat information crimes, Law No. 2 of 2006.
- **Egypt's Information Crimes Project**: Egypt's legislation aims to safeguard information transmission and exchange through laws on communications and electronic signatures.

TopicTwo: Protection Methods Against Online Fraud Crimes

This section discusses methods of protection against online fraud, beginning with the first subsection, which defines electronic fraud, and the second subsection, which highlights key protection methods against online fraud.

subsection One:

Definition of Electronic Fraud

Fraud is defined as: the crime that is achieved when the offender or someone else acquires movable property owned by another person without right, as a result of the offender using one of the means of deception specified by law, which causes the victim to be misled into handing over the property (Al-Azzawi, 2004, p. 638).

As for online fraud, it is defined as: any act of pretense or suggestion that misleads the victim in a way that leads to a direct belief in the external appearance of the fraud. This means that the victim in online fraud is someone who has fallen for the deception of the perpetrator using a computer and the internet, thereby being misled and handing over money (Al-Shawabka, 2004).

Online fraud does not only target natural persons but can also apply to legal entities, such as public institutions, companies, and private organizations, which are considered legal persons

under the law. Since computer systems and internal networks of organizations are branches of the institution or company, they can also be the target of fraud or deception (Al-Ubaidi, 2010).

subsection Two:

Main Methods of Protection Against Internet Fraud Crimes

Some studies address several methods to combat electronic crimes, most of which are widely used in many countries, especially in the Gulf Cooperation Council countries. These methods include:

1. **Passwords**: Without passwords, no unauthorized person can access the information network. A password proves that you are authorized to access the network, and it is one of the simplest ways to protect information. When creating a password, a few key points must be considered: it should be complex, consisting of a mix of numbers and letters, difficult to guess, kept confidential, and changed regularly.
2. **Firewalls**: A firewall can be either a program or a device equipped with software used to protect a network and server from intruders. Firewalls operate in various ways, depending on the type of firewall and the network it protects, according to the institution's policy. Some of these methods include:
    - Packet Filtering: Screening data packets sent across the network.
    - Envelope Filtering: Changing the destination addresses of envelopes coming from the internal network.
    - Stateful Inspection: Monitoring the state of the traffic flow.
3. **Automatic Updates**: Continuous and automatic updates of software and operating systems are essential for protecting information networks. Companies constantly work on improvements to fix weaknesses in software and systems. These improvements are always available in updates, and most software manufacturers have added the automatic update feature, allowing the system to periodically connect to the manufacturer’s server and download the latest updates automatically.
4. **Encryption**: Encryption means encoding data in a way that prevents it from being read by anyone who does not have the password to decrypt it. Encryption keys are used to encode the transmitted texts and decode them by the rightful owner who is authorized to receive the data. The strength and effectiveness of encryption depend on the type of algorithms used.
5. **Backups**: Backing up the content of computers or information networks and storing these backups in a secure place far away ensures that they can be retrieved in case of a system failure, network disasters, or any other cause that leads to data destruction (Al-Maliki, 2015, p. 82-85).

Topic Three

Penalties for Online Fraud Crimes in Saudi Law

The Kingdom of Saudi Arabia places significant importance on combating online fraud crimes by enacting strict legislation aimed at protecting individuals and institutions from cyber threats. The Cybercrimes Law, issued by Royal Decree No. (M/17) on 8 Rabi' al-Awwal 1428H (March 26, 2007), provides a clear legal framework for criminalizing unlawful acts committed via the internet, with penalties established based on the seriousness and impact of the crime on national, economic, and social security. Online fraud crimes are among the most significant challenges

facing Saudi society, due to their negative impact on digital trust and financial stability, prompting the imposition of stringent penalties to curb their spread.

This chapter will examine, in Section One, the definition of these crimes according to Saudi law, in Section Two the penalties assigned, in Section Three the legal mechanisms used to combat electronic fraud, and Section Four will analyze the challenges and future efforts the Kingdom is working on to enhance this area.

subsection One:

Definition of Online Fraud Crimes in Saudi Law

The Cybercrimes Law defines electronic fraud as any act committed using a computer or an information network with the intent to unlawfully acquire movable property, legal documents, or to obtain an illicit benefit for oneself or others by means of fraud, impersonation, or providing misleading information. This definition includes several illegal activities, such as using fake websites to deceive users, stealing payment data, or impersonating others to gain unauthorized financial benefits (Law on Combating Financial Fraud and Breach of Trust, Royal Decree No. (M/79), issued on 10/9/1442H).

subsection Two:

Penalties for Online Fraud Crimes

The law imposes strict penalties on those who commit online fraud, depending on the severity of the crime and its impact on the victim and society. Article 4 of the Cybercrimes Law mandates imprisonment for up to three years for those engaged in electronic fraud aimed at illegally acquiring others' funds, such as manipulating websites or creating fake platforms to collect money without just cause. A fine of up to two million Saudi Riyals, or imprisonment, or both, is also imposed on anyone who impersonates another person online for financial gain or to deceive others into making illicit profits. In the case of repeated offenses or crimes committed by a public employee or someone working in a sensitive position, the penalty is doubled according to the law, with the confiscation of all proceeds from the crime and a requirement for the offender to return the stolen money to the victims and compensate them for any material or moral damages caused by the fraud (Cybercrimes Law, Royal Decree No. (M/17), dated 8 Rabi' al-Awwal 1428H).

In some cases, the penalties are harsher. For instance, when online fraud crimes threaten national security or destabilize financial systems, stricter penalties are applied to reflect the severity of the offense. Organized financial fraud via the internet, especially if it targets a large number of victims or extends to government agencies or major financial institutions, can result in imprisonment for up to ten years and a fine of up to five million Saudi Riyals. The use of advanced technology, such as artificial intelligence or malicious software, to carry out fraud is considered an aggravating factor, leading to harsher penalties. Furthermore, defrauding government entities or legal personalities results in penalties that exceed the maximum limits, with additional measures to prevent reoffending (Cybercrimes Law, Royal Decree No. (M/17), dated 8 Rabi' al-Awwal 1428H).

subsection Three:

Legal Mechanisms to Combat Online Fraud Crimes

The concerned authorities in Saudi Arabia work effectively to apply penalties through integrated legal and procedural mechanisms, including tracking suspicious financial transactions in coordination with banks and regulatory bodies to ensure the detection of illegal activities and the prosecution of offenders. There is also international cooperation to pursue fraudsters who use the

internet to defraud Saudi citizens from outside the Kingdom, where information and data are exchanged with relevant authorities in other countries to facilitate the apprehension of perpetrators. Saudi courts rely on digital evidence in trials, analyzing electronic data and digital communications to prove the involvement of offenders, ensuring justice based on reliable evidence. Public awareness campaigns are also launched to educate individuals and companies on common fraud methods and ways to protect themselves, including caution about suspicious links and verifying the credibility of websites before conducting any financial transactions (Al-Sulaimani, 2024).

subsection Four:

Challenges and Future Efforts

Despite the stringent legislation, online fraud crimes continue to evolve, with fraudsters constantly seeking to exploit technological gaps and security breaches. Therefore, the Kingdom is working to continuously update its laws to keep pace with new fraudulent methods, while also enhancing international cooperation to combat cybercrimes. The Kingdom is also developing artificial intelligence techniques to detect fraudulent activities before they occur and strengthening the capabilities of specialized security agencies in handling digital investigations and analyzing cybercrimes professionally.

In conclusion, penalties for online fraud crimes in Saudi law are among the strictest in the region, aiming to deter offenders and protect individuals and institutions from the risks associated with these crimes. Through the enforcement of stringent laws, enhancing cybersecurity, and raising societal awareness, the Kingdom seeks to create a safe digital environment that minimizes opportunities for fraudsters and strengthens trust in the digital economy, reflecting its commitment to ensuring national, economic, and social security amid rapid digital transformation.

Conclusion:

With the increasing reliance on technology and the internet in various fields, online fraud crimes have become a real threat to individuals, institutions, and nations, necessitating the establishment of clear legislation and effective mechanisms to combat them. This research has addressed the concept of cybercrimes from various legal perspectives, reviewing the different definitions of these crimes in Saudi laws and international statutory laws, while highlighting their reality in the Kingdom of Saudi Arabia and the risks they pose to national security, as well as ways to confront them. The research also analyzed the legal challenges related to online fraud crimes and the penalties imposed on offenders according to both Saudi and international legislation.

Based on the findings presented in the chapters of this research, the first section will focus on presenting the key conclusions reached. The second section will provide a set of recommendations that could enhance efforts to combat these crimes.

Section One

Findings

This research has concluded a number of results that reflect the reality of online fraud crimes.

First, it is clear that online fraud crimes have become one of the most dangerous modern crimes threatening national, economic, and social security, due to their complex nature and their ability to cross borders, making them more difficult to combat compared to traditional crimes. The increasing reliance on technology in all aspects of life has expanded the scope of these crimes, so

that they no longer only include online fraud, but also cover electronic espionage, blackmail, privacy violations, and hacking of digital systems.

The study revealed that Saudi laws are among the most advanced in the region in dealing with online fraud crimes, as the Cybercrime Law specifies deterrent penalties for various types of cybercrimes, including online fraud, privacy violations, system breaches, and electronic defamation. However, legal challenges remain in facing these crimes, especially with the evolution of methods used by criminals to exploit technical vulnerabilities and evade legal punishments.

The study also highlighted those international legislations, such as the Budapest Convention on Cybercrime, provide an important legal framework to face cyber threats. However, the differences in laws between countries hinder effective cooperation in pursuing criminals who commit online fraud across borders.

One of the key findings of the research is that online fraud crimes do not only target individuals, but have increasingly become a threat to financial institutions and government bodies, necessitating the enhancement of cybersecurity as a top priority to protect information and digital systems. It was also found that raising public awareness about the dangers of online fraud is a key element in reducing these crimes, as many online fraud operations succeed due to a lack of awareness about digital protection methods.

Regarding the penalties for online fraud offenders in Saudi Arabia, the research confirmed that the penalties set out in the Cybercrime Law are deterrent, with some penalties reaching up to ten years in prison and fines of up to five million Saudi riyals, reflecting the seriousness with which these crimes are dealt. However, despite this, the research highlighted the need for continuous updates to laws to keep pace with new methods used by criminals to commit online fraud.

Section Two

Recommendations

Based on the findings of this research, a set of recommendations can be made to enhance efforts to combat online fraud crimes and improve legal and technical frameworks for addressing them.

First, continuous updates should be made to Saudi legislation to keep up with the rapid developments in online fraud crime techniques, ensuring that legal loopholes that criminals may exploit to carry out their operations without facing legal consequences are closed. Updates should also include harsher penalties for online fraud crimes targeting national infrastructure and government agencies, as these crimes pose a direct threat to national security.

International cooperation should be strengthened in combating online fraud crimes by signing information exchange agreements between Saudi Arabia and other countries and joining international initiatives such as the Budapest Convention on Cybercrime, which facilitates the pursuit of criminals who carry out online fraud operations from outside the Kingdom. Coordination between the Gulf Cooperation Council (GCC) countries should also be enhanced to establish a unified legal framework for combating online fraud crimes and exchanging expertise in cybersecurity.

On a technical level, investment should be made in developing artificial intelligence techniques to detect fraudulent operations before they occur and to establish advanced security systems capable of proactively countering cyberattacks. The role of the National Cybersecurity Authority should also be enhanced in protecting digital infrastructure by developing advanced security

policies and providing technical and logistical support to both government and private sectors to ensure the security of their information against breaches and online fraud.

Public awareness campaigns are one of the most important tools in combating online fraud crimes. Therefore, campaigns should be launched targeting individuals and institutions to educate them on online fraud techniques, ways to protect against digital breaches, the importance of using modern protection software, and the risks of sharing personal data online with untrusted entities. Furthermore, cybersecurity modules should be included in educational curricula to raise awareness among future generations about the dangers of the internet and how to protect themselves from it.

Finally, it is essential to strengthen cooperation between the public and private sectors to combat online fraud crimes. Companies and financial institutions should work together with security and legislative authorities to exchange information about fraud attempts and cyber breaches, contributing to the creation of a more integrated and effective security system. Encouraging scientific research in the field of cybersecurity and developing local solutions to combat digital crimes is also necessary to keep up with technological advancements in this field.

This research was founded by the General Directorate of Scientific Research & Innovation, Dar Al Uloom University, through the Scientific Publishing Funding Program.

References

1. Abdullah, A. (2018). *Cybersecurity and electronic crimes*. Riyadh.
2. Abdullah, A. (2018). *Digital communication tools and their impact on modern societies*. Riyadh: Media Studies Center.
3. Abu Ghulayon, A. M. (2009). *Electronic crimes between Islamic Sharia and positive laws* (Master's thesis). Jordan University, Graduate Studies College, Jordan.
4. Al-Azawei, E. H. A. (2004). *Fraud crime in Iraqi law* (1st ed.). Baghdad: Al-Sabah Publishing & Advertising Office.
5. Al-Bedawi, A. T. (1432 AH). *Internet, Bluetooth, Blackberry, and extortion crimes*. Dammam: King Fahd National Library Cataloging.
6. Al-'Otaibi, M. (2023). *Everything you need to know about combating electronic crimes and their importance*. Retrieved from https://mohammedalotaibi.sa/
7. Al-Mana'asa, A., & Al-Zoubi, J. M. (2001). *Computer and internet crimes: A comparative analytical study* (1st ed.). Dar Wael for Publishing, Amman.
8. Al-Salem, M. M. (2013). *Electronic crimes in Palestinian legislation: A comparative analytical study* (Master's thesis). Islamic University – Gaza, Faculty of Sharia and Law, Palestine.
9. Al-Thunayan, T. N. (2012). *Proving electronic crime: A theoretical and applied study* (Master's thesis). Naif Arab University for Security Sciences, Graduate Studies College, Riyadh.
10. Al-Zaiyadi, F. H. (2011). *Electronic crimes and the internet*. Information Technology Journal, Issue 36.
11. Al-Zoubi, M. A. (2004). *Computer crimes and internet crimes: Information crimes*. Amman: Dar Al-Thaqafa for Publishing & Distribution.
12. Al-'Azawi, I. H. A. (2004). *Fraud crime in Iraqi law* (1st ed.). Baghdad: Al-Sabah Publishing & Advertising Office.

13. Al-Momani, N. A. (2008). *Information crimes*. Dar Thaqafa for Publishing & Distribution, Amman.
14. Al-Turaiki, A. A. (n.d.). *National security: Concept and dimensions*.
15. Al-Fitih, M. E. (2024). *Learn about the punishment for electronic crimes in Saudi Arabia*. Retrieved from https://sul-aza.com/punishment-for-cyber-crimes
16. Al-'Otaibi, M. (2023). *Everything you need to know about combating electronic crimes and their importance*. Retrieved from https://mohammedalotaibi.sa/
17. Ayad, M. (2007). *Criminal protection in national legislations and international cooperation*. Dar Al-Nahda Al-Arabia.
18. Ayad, M. (2024). *Criminal liability in cybercrimes*. (2nd ed.), Issue 39.
19. Ibn Manzur. (1994). *Lisan al-Arab*. Dar Sader, Beirut.
20. Mahjoub, M. S. (2004). *The roots of crime and punishment*. Cairo: Arab Thought House.
21. Mohamed, M. F. (2023). *Cybersecurity strategy in Saudi Arabia*. National Competitiveness Center. Retrieved from https://www.ncc.gov.sa/ar/
22. Maktabi, S. H. (2009). *Modern trends in computer fraud crime*. Saudi Law Review, 22(2), King Saud University.
23. Saudi Cybercrime Law (2007). *Cybercrime Law of the Kingdom of Saudi Arabia* (Royal Decree No. M/17, March 8, 1428 H). Retrieved from https://laws.boe.gov.sa/
24. Rania, M. (2023). *Mechanisms to combat cybercrimes in Saudi Arabia: An analytical study*. Legal Journal, 15(5).
25. Wael, M. N., & Ghada, A. R. (2018). *Online fraud via the international information network: A comparative study of Saudi and Jordanian law*. Journal of Political and Legal Studies, 19.