AL-BIRUNI

Al-Biruni Journal of Humanities and Social Sciences
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900
https://al-biruni-journal.jo

The Scene of Electronic Fraud Crimes: A Comparative Study of Jordanian and Spanish Legislation

MAJED FALAH ALSARHAN[1], NADER QASIM MOHAMMAD ALSARHAN[2]

[1] Assistant Professor, criminal law, Zarqa University, Jordan, Zarqa, Email: malsarhan@zu.edu.jo
[2] Assistant Professor, Department of Political Science, Faculty of Law, Jadara University, Jordan, Email: n.alsarhan@jadara.edu.jo

* Corresponding Author: MAJED FALAH ALSARHAN, malsarhan@zu.edu.jo

DOI: https://doi.org/10.64440/BIRUNI/BIR009

ARTICLE INFO

Article history
Received Oct 12, 2025
Revised Oct 13, 2025
Accepted Nov 14, 2025

Keywords
Electronic Fraud Crimes;
Jordanian legislation;
Spanish Legislation.

ABSTRACT

This is comparative have a look at among the Jordanian and Spanish Legislation of the Location of Electronic Fraud Crimes. This studies sought to have a look at the strengths and weaknesses of present day Jordanian regulation and Spanish regulation. The look at observed disparities in some elements between them, that are predicted, as they belong to one of a kind felony cultures and felony systems. The examine endorse that :to Prompt collaboration and coordination among numerous organizations and jurisdictions with various priorities, Advocating for the allocation of country wide and global resources for legislation and the enforcement of cyber fraud ,Improving legislation with the aid of integrating improvements that enhance the effectiveness and performance of codes so that you can sell transparency and responsibility ,Providing everyday education for staff to understand the complexities of fraud, which includes in IT, language, and electronic funding, Directing regulatory bodies to proactively pick out and mitigate the impact of digital fraud assaults and Encouraging public-non-public partnerships to elevate focus approximately the dangers of digital fraud and shield investments and assets.

This is an open-access article under the CC–BY-SA license.

1. Introduction

The rapid development of records and verbal exchange technology has fundamentally reshaped modern society, enabling new forms of financial interaction, negotiation and service transport. However, these advances have also created fertile ground for the rise of electronic fraud, which has become one of the most widespread and sophisticated types of cybercrime. Electronic fraud exploits vulnerabilities in virtual structures, electronic transactions and statistical systems, and poses a major risk to nationwide security, monetary balance and public trust (Shulzhenko and Romashkin, 2020).

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

As Internet use will increase and digital offerings come to be more integrated into every day life, fraudulent sports along with online identification theft, phishing schemes and unauthorized manipulation of information have end up more and more good sized. These unlawful practices affect now not best individuals but additionally financial establishments, non-public companies and public our bodies. Previous studies show that electronic fraud is shaped by means of each technological and behavioral factors, making it hard for regulatory systems to maintain pace with their evolving practices (Ololade et al., 2020; Tambe et al., 2024).

It has consequently grow to be essential for coverage makers and crook justice structures to recognize the concept, scope and remedies of electronic fraud. Countries vary of their felony tactics, enforcement talents and judicial interpretations of cybercrime. For instance, Jordan has introduced a number of legislative measures to modify cyber sports and cope with digital fraud, but it still faces challenges associated with the modernization and harmonization of its prison framework (Khater et al., 2024; Jalghoum et al., 2021). Spain, alternatively, has developed a more dependent felony framework shaped by using EU directives and worldwide conventions, permitting it to set up extra complete mechanisms to combat electronic fraud (Volobuiva et al., 2023; Sagir and Kafurtanis, 2022).

Given the worldwide and borderless nature of digital fraud crimes, it turns into vital to compare countrywide criminal structures to become aware of shortcomings, strengths and possibilities for prison reform. The reason of this look at is to evaluate Jordanian and Spanish regulation concerning the crime of digital fraud, and spotlight how each country Defines, criminalizes and prosecutes those crimes. Through this comparative lens, the research seeks to provide insights which could assist the improvement of more effective felony frameworks capable of meeting the growing challenges posed via electronic fraud in each countrywide and international contexts.

1.1. Research Problem

Despite the growing prevalence of electronic fraud and the growth of digital technologies in Jordan and Spain, giant gaps continue to be inside the clarity, comprehensiveness and enforcement of the existing felony framework. The main trouble this look at addresses is:

To what volume do the Jordanian and Spanish criminal systems correctly define, modify and prosecute electronic fraud, and how do differences in legislative procedures have an effect on their capacity to reply to the evolution of this crime?

1.2. 2. The Concept of Electronic Fraud Crimes

The phenomenon that has increased inside the cutting-edge records age is globalization. This international motion has given rise to many useful adjustments, fostered relationships between humans and facilitated the exchange of thoughts and subculture, as well as casting off geographical obstacles. Unfortunately, this worldwide have an impact on has also

resulted in lots of harmful adjustments. A good sized alternate involves the global unfold of fraud, particularly electronic fraud. As a end result, prison frameworks need to be flexible to deal with the growing scope of conflicts, consisting of criminal ambiguities arising from the global nature of digital fraud. (Ololade et al. 2020).

The upward thrust of electronic fraud is a end result of the unlimited possibilities of information and communique technologies, which has led to the improvement of latest concepts including Internet fraud and e-fraud. The dynamic nature of these illegal acts requires non-stop updating of the law to deal with new paperwork and techniques. Electronic fraud operations are becoming increasingly extensive and might have some distance-achieving outcomes for society. It isn't handiest the sufferers who're centered, but additionally the manner people stay and eat, which ends up in interdisciplinary results. Those worried in pc fraud, including those answerable for deciphering the law, are tasked with protecting privacy and keeping ethical requirements. (Tambe et al. 2024).

The scale of fraud devoted through statistics and communication systems and networks is specially tremendous because of technological advances, that have expanded crook opportunities. It is not limited to external computer professionals, but additionally includes using easy laptop equipment that don't require substantial know-how. A massive wide variety of human beings in numerous sectors are worried in unlawful sports on the Internet. In the past, e-commerce fraud by and large involved deceptive advertising, together with counterfeit, stolen, pirated or substandard items. Some of these accessories are deliberately designed to fail or purpose harm during use. Illegal on line buying and selling practices include phishing attacks, spam mail and on line pharmacy scams, wherein websites offer prescribed drugs without a prescription from a professional. There is terrific situation amongst professionals that these crook sports ought to attract terrorists who seek funding and purchase weapons. Apart from organising the definition of cybercrime and taking punitive measures, handling electronic fraud is a extra complicated undertaking. Given the tremendous nature of electronic fraud, this take a look at pursuits to consciousness at the locations in which electronic fraud happens. (Razaq et al. 2021).

1.2.1. The reviewed literature suggests that maximum definitions of electronic fraud consciousness usually on its technical dimensions, yet do not completely seize the socio-criminal complexities that have an impact on legislative responses. A important evaluation shows that law frequently lags in the back of technological innovation, resulting in regulatory loopholes that criminals take advantage of. Furthermore, the multidisciplinary nature of electronic fraud – combining technological, financial and behavioral factors – requires a more integrated prison strategy than visible in many jurisdictions, consisting of Jordan and Spain.

1.2.2. 2.1. Definition and Scope

This phase provides a systematic survey of electronic fraud, consisting of a class of these crimes and their actual occurrences. Electronic fraud differs from behaviors which includes

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

electronic counterfeiting and electronic misuse of services, both of which can result from fraudulent activities through electronic devices. (Malik et al. 2022).

Fraud refers to criminal sports that involve the misuse of era, consisting of credit score card fraud, identification theft, and fraudulent schemes. All those sports contain the manipulation of private information. Electronic fraud includes the unauthorized acquisition, alteration or distortion of data, specially within the case of digital transmission of statistics in which weaknesses in communique networks are exploited. The economic effect of on line fraud is enormous, with weekly losses predicted at $1.7 million and character companies doubtlessly losing extra than $10 million to such fraud. (Stapleton, 2022).

The act of electronic fraud involves the unauthorized or felony acquisition or disclosure of any other's electronic belongings for private gain. This form of fraud makes use of advanced technology to accumulate or transfer electronic assets with out consent, resulting in a monetary gain for the criminal and loss for the rightful proprietor. In Finland, electronic fraud legal guidelines have been prolonged to cowl altered digital messages and their deletion or alteration.

Similarly, the Fraud Act 2006 in the UK addresses electronic fraud with the aid of which include fraud, deception or breach of trust, and redefines fraud as digital deception. There is an worldwide trend advocating a change inside the prison definition of fraud to encompass digital fraud, now not simply acts and verification of beyond acts. This have a look at seems at electronic fraud legal guidelines in unique international locations to evaluate and endorse new recommendations for electronic fraud. The policy targets to conform country wide laws to global values and efficiently cope with electronic fraud. The take a look at additionally examines the criminal standards, evidence and rights in electronic fraud cases, even as recognizing the diverse nature of those crimes. As digital fraud technologies and tactics keep to evolve, it is crucial for the ones concerned in managing these crimes to stay informed and adapt legislative content accordingly. (Cole, 2023)

1.3. 3. Legislation on Electronic Fraud Crimes in Jordan

The most crucial criminal documents related to fraud within the Jordanian judiciary include the Criminal Code, the Draft Law on Information System Security, the Law on Misuse of Digital Signatures and Intellectual Property and other laws associated with on-line gambling. According to the Criminal Code, "fraud" is described as a particular type of fraud regarding the usage of electronic computer systems or interconnected networks. Jordanian law addresses the difficulty of "fraud", underneath Part Two of the Penal Code, "Crimes towards Property", which specifically pertains to obtaining cash through the exploitation of pc structures or interconnected networks. The development of the Criminal Code in 1978 was primarily based on Yugoslavia's legislative version, at a time while laptop technology changed into now not enormous in Jordan. Subsequent modifications to

the Criminal Code were made up to 2008, reflecting the growing importance of addressing criminal activities in cyberspace. In 2007, a new regulation become drawn up to fight electronic fraud, even as current fraud provisions inside the penal code have been retained below the segment "Computer crime". This demonstrates the evolving method of the Jordanian legislature in addressing this unique crime within the legal framework. (Khattar et al. 2024).

A crucial evaluation of Jordan's prison framework suggests that tremendous development has been made in updating cybercrime legal guidelines, but the legislative reaction stays reactive in preference to proactive. Relying on amendments as opposed to comprehensive legislative restructuring limits the regulation's adaptability to new fraud strategies. In addition, ambiguity in criminal definitions and overlap between several laws can prevent steady felony interpretation and weaken enforcement mechanisms.

1.3.1. 3.1. Overview of Jordanian Legal Framework

In recent decades, many laws and regulations have been introduced to keep pace with the development of information technology and deal with various forms of cybercrime. The most important law in this area is the Information Systems Act, which was adopted in 1995 and later amended in 2009. This law, in combination with other laws such as the E-Transactions Act issued by decree in 2001 and later amended in 2011, as well as authentication provisions, addresses a wide range of information technology, communication equipment and transactions. permission of electronic data and personal matters. It also outlines the offences, liability and penalties for unauthorized access to information systems and networks. In addition, legal texts regulate unauthorized, illegal and harmful exploitation of privacy without consent. (Nukusheva et al. 2022)

Derived from the Jordanian Information Systems Law of 1995, these regulations are considered a thorough and beneficial framework for overseeing the IT industry in society. Mainly focused on handling electronic records, digital certificates, audio, video and digital documents used by public entities to streamline processes, the law has become outdated with a lack of technological advances hindering its implementation. The analysis will also explore the interpretation of electronic crimes by Jordanian judges and public prosecutors, which will shed light on the effectiveness of the laws in combating electronic fraud. Furthermore, the paper will compare these legal provisions with international standards and European laws relating to electronic fraud criteria. Beginning with a discussion of these laws and trends, the article will also address the evolution of processes and reforms, including e-signature legislation, that aim to address these limitations but ultimately fall short of the necessary requirements. (Jalghaum et al. 2021).

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

1.4. 4. Legislation on Electronic Fraud Crimes in Spain

Law 10/1988, dated May 7, regulating the jurisdiction of minors in criminal cases, was the first legal document in Spain to address crimes related to new technologies. Although Law 10/1995, adopted on 23 November, regarding the Criminal Code covered some criminal behaviour, issues such as specific types of crimes, the perpetrator's intent and sentencing were not adequately addressed. As a result, Spain had to update and modernize its criminal code in order to effectively prosecute this type of crime. In response to the risk and new criminal phenomena in society, the new Spanish Penal Code entered into force on July 1, 1996. Title XIII, "Crimes against public administration, administration of justice and legal documents", contains provisions aimed at protecting the security of financial transactions and establishing mechanisms for coordination between community institutions that serve different purposes. The purpose was to incorporate into Spanish law norms that criminalized these new types of crimes. In particular, Article 288 of the Criminal Code imposes a penalty for issuing a check without sufficient funds.

Society's development towards a global communication and information society with advances in all aspects of life and work has given rise to various new forms of criminal activities using new technology. In this social context, the crime of electronic fraud is addressed in the Spanish Penal Code of 1995. Considering the specific concerns related to electronic fraud and the threats to the interests concerned, a comprehensive investigation of electronic fraud and procedures to investigate such complex cases have been presented. (Volobueva et al., 2023).

The Spanish Penal Code of 1995 emphasizes the protection of the jurisdiction of courts and tribunals against electronic fraud. It is outlined in Chapter VI of Title XIII, which covers "Crimes against public administration and the administration of justice and management of legal documents". Electronic fraud is classified as a type of abuse or fraud as well as bankruptcy. The code specifically deals with the fraudulent alteration of telecommunications or original chips, which includes penalties of one to five years in prison and a fine of twelve to twenty-four months. In cases where the change in portability for financial gain harms a third party, the penalty increases to two to five years. Fraudulent use of telecommunications terminal equipment or loss as a result of hostile action is also punishable. The Spanish Criminal Procedure Code regulates the application of these crimes, including the appointment of expert witnesses and evidentiary aspects. Expert testimony in electronic fraud cases involves analysis of the relevant legal framework and detailed investigation. The Social Chamber in the Supreme Court presents specific criteria for evidence assessment, including the distinction between recommended and non-recommended evidence processing. Expert testimony in electronic fraud cases examines the reality that has been assessed to uncover the essentials of the claim. (Saghir and Kafartanis2022).

1.4.1. 4.1. Overview of Spanish Legal Framework

Existing legal texts that contain specific rules related to online fraud include the Protection of Citizens or the Law of Civil Protection, the Spanish Penal Code, the Organic Law on the Protection of Personal Data, the Organic Law on the Regulation of Organizational Law and the Organic Law on Private Security. Although these texts do not classify many acts as cyber fraud, the recent proposal for the Law on the Protection of Personal Data and the Guarantee of Digital Rights integrates the Directive on attacks against information systems, resulting in a reform of the criminal law. In addition, a preliminary draft reform of the Private Security Act is currently under discussion. (Baechler, 2020)

By organising these criteria, we will therefore assess whether or not the government in Jordan and Spain are thinking about a specific behavior or, if vital, intend to take legal movement. However, earlier than proceeding, it's miles vital to offer an overview of the legal framework in Spain. The dialogue of Spanish law referring to assaults on statistics systems includes addressing the relevant provisions of the Spanish Penal Code. Researchers have stated that Spain was one of the first European international locations to feature cybercrime offenses to its criminal code, together with the advent of malware, in the early 2000s. Despite a sluggish start, Spain has made full-size progress in coping with this trouble, developing a robust legal and procedural framework adapted to the modern-day social challenges within the vicinity. (Оразхан & Татаринов2020)

1.5. 5. Comparative Analysis of Jordanian and Spanish Legislation

It is crucial to thoroughly take a look at the legal guidelines in Jordan to fight electronic fraud. In addition, it's far prudent to have a look at the legal framework of every other jurisdiction to assess the effectiveness of existing law. The hobby in Spanish law stems from the united states of america's geographical area, its compliance with legal guidelines set by the European Union and international businesses, and the cultural, economic and social characteristics shared among Spain and Jordan. This consists of the ancient interplay among Christians, Jews and Muslims, the extensive Muslim and Arabic-speaking populations in each international locations, and their modern attitudes in the direction of new technologies. Therefore, our examination of Spanish crook regulation will encompass the nature of electronic fraud and its definition, the criteria for setting up criminal legal responsibility, the penalties for criminal conduct, the companies answerable for imposing these penalties, Spain's legal mind-set to fraud within the context of global crime, and the potential for enhancing the effectiveness of criminal coverage in the country. (Toubat et al., 2020).

Comparing the social elements of both jurisdictions, Spain has taken measures to guard its pc systems, infrastructure providers and economic system. These measures consist of joining the Cybercrime Convention and the Computer Emergency Preparedness Team. This textual content outlines three steps for a complete analysis of Spanish law enforcement to fight fraud:

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

1. Examination of Spanish criminal regulation, such as the definition of digital fraud, the overall law of fraud and its aids, the relevant articles on serious fraud and the corresponding sanctions underneath Spanish criminal regulation.

2. Evaluation of the real implementation of confiscation of proceeds from digital fraud.

3. To gift findings and pointers to lessen euro fraud. (Chaves-Avila and Gallego-Bono, 2020).

A deeper evaluation shows that each Jordan and Spain proportion structural weaknesses in managing the transnational nature of digital fraud. However, Spain advantages from EU-huge harmonisation, even as Jordan's felony reforms are largely domestic and fragmented. This difference drastically influences the consistency and effectiveness of enforcement. Furthermore, Spain's jurisprudence affords more specific felony interpretations, while Jordan is predicated closely on prison texts with constrained case regulation analysis.

1.5.1. 5.1. Key Similarities and Differences

In this section, we will examine important comparative data between Jordanian and Spanish PCs, as well as differences between the two countries, in order to propose penal measures to punish electronic fraud. We have identified and discussed a number of similarities, important differences and nuances between Spain and Jordan in terms of legislation against electronic fraud and the methods used to prosecute such cases. A. Similarities: Both Jordanian and Spanish legislators agree that severe penalties should be applied to persons found guilty of electronic fraud, with the aim of eliminating this deliberate form of crime. Both legal systems require the establishment of comprehensive regulatory frameworks to effectively address new technologies within their scope. This suggests that the perception of fraud is influenced by various cultural and legal factors. While the act of new provisions in this area may indicate legislative control with speculation about future developments in criminal law, it can also be seen as a positive development.

The Spanish legal gadget makes use of a large interpretation to apply new rules to antique technological phenomena, often enforced by using worldwide treaties and conventions. B. Differences: The Jordanian courts often used Articles 40 and one hundred and five of the ACC to prosecute and punish fraud-related offenses. It is noteworthy that those Articles are contained in three exclusive laws. However, while digital information structures are involved in fraud or forgery, Articles fifty four and 167 of the Telecommunications Law are used to criminalize fraud and punish offenders. Additionally, No. 13/1995 and Article 12 of the Computer Misuse and Cyber Crimes Act also are criminally punishable. It is important to bear in mind the enforcement mechanisms used in each jurisdictions. Unlike Spain, the use of Class 2 mechanisms in Jordan will necessarily restriction and prevent the intentional fee of electronic fraud. (Al-Qaaida, 2021)

1.6. 6. Case Studies and Examples

"Dhahir," a 35-year-old Jordanian engineer, utilized hacked smart weapon units, vehicle plates, and entrance cards to manipulate the outcome of the competition between the Jordanian Army and a select group of elite individuals. This resulted in a victory for the village's second-class football team against the Jordanian Army football team, which took place while the Jordanian King was present to boost the morale of the army players before the match. Following a trial in accordance with Jordanian law, "Dhahir" was found guilty but his 6-year sentence was reduced to 5 years due to his good behavior during the investigation and trial. As part of the verdict, "Dhahir" was also ordered to pay 5,040 JD to the Jordanian government, an amount equal to 224% of what he stole, despite the fact that the Jordanian Penal Code allows for compensation to be paid to the government of three times the stolen amount for each fraudulent crime committed. (Madi & Malhas, 2024)

At the age of 24, a Sudanese citizen named "Selim" obtained a large amount of fake or unauthorized email accounts, names, addresses, credit cards, bank account numbers, passport numbers, laptop serial numbers, and Internet Protocol addresses from various online sources. Selim used this information for illegal activities on the internet, including sending emails with viruses or malware to victims, once he had confirmed the accuracy of the data. At 19, "Selim" was found guilty by a court in Jordan and given a ten-year prison sentence for wrongfully manipulating other people's computers, producing fraudulent electronic content, selling such content, engaging in criminal impersonation, and conducting money laundering. After serving five years of his sentence, he was deported and put on a list of suspected repeat offenders. When he arrived at Queen Alia Airport in Amman, "Selim" was questioned by the police, claiming that he had been falsely accused in the past and that he had changed his ways by abandoning criminal activities. However, following further investigation, the police arrested him later that evening after he was caught using a fake bank card to withdraw money from another person's account. Both he and the seller of the fake card, who had been involved in several other electronic fraud cases, were subsequently sentenced to ten years in prison by the relevant Jordanian court. (Abu Sarhan & Fouché)

In 2006, an individual known as "Legaz" established connections with high-ranking officials at several major Spanish national banks, including the Bank of Castilla, the Caja de Ahorros y Monte de Piedad La Caja de Castilla-La Mancha, the Bank of España, and R.M.S Opinno Capital. "Legaz" falsely assumed the identity of the Secretary of the Board of Directors of the Bank of Castilla and posed as an Interpol officer. He was also among the initial 900 investors in the "Top Funds" project, which was managed by Opinno Capital. "Top Funds" was a collaborative investment venture between a leading cybercrime coping company and a renowned mutual fund management company based in Spain. Records show that between 2007 and 2010, "Top Funds", led by "Legaz", invested 25,124,795.21 EURO in 27 different computer security software projects. Only one conviction has been secured to date under the existing Spanish electronic fraud laws, in

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

case: 2-2008, by the National Police in Madrid. A year ago, the Public Prosecutor's office sought a 16-year prison sentence for the leader of the "Nationalist-Patriotic Criminal Group Pravda", and 15 years for each of his 3 associates. The presiding judge at the Central Penal Court number 19 in Oviedo has requested a 30-year prison term for "Legaz" and his partner, who are accused of perpetrating electronic fraud as computer saboteurs and organizers of phishing activities. (Baechler, 2020)

1.7. 7. Challenges and Future Directions

In Spain and Jordan, there are unique challenges that require attention and action, despite the varying circumstances. Updating rules associated with era offers a good sized obstacle. Combating electronic fraud relies upon on not simplest enhancing neighborhood laws and technical capabilities, however also on instructing the general public about ability risks and how to mitigate them. Though this look at did no longer delve into these problems, policymakers and decision-makers want to take them under consideration when revising or developing technology-related laws. Subsequent research have to embody these elements whilst examining various varieties of technology-associated crimes. (Svensson-Hoglund et al.2021)

Another important challenge lies in the continuous development of technologies. Cooperation at international level is necessary to reduce the negative effects of this problem. This cooperation may include cooperation between mobile service providers. The National Commission for the Telecommunications Market and Competition in Spain has identified two mobile service providers that have an unacceptable impact on network neutrality by blocking Voice-over-Internet-Protocol (VoIP) technologies that offer free mobile phone calls. As a result, the Commission has ordered that both companies have a period of one month to deal with the unacceptable impact caused by the blocking of VoIP services. During this time, companies are also required to inform their customers that they are blocking these services and also provide them with instructions on how to unblock them. This case underscores the importance of implementing additional measures to promote cooperation between mobile service providers and law enforcement agencies responsible for combating cybercrime. (Trivino et al. 2020)

In accordance with the effects of this look at, there are several vital measures that need to be implemented in the future. First and essential, it's far crucial to adjust the relevant laws to maintain tempo with technological advancements. Additionally, regulation enforcement organizations liable for addressing cybercrimes in each international locations need to enhance their collaboration and cooperation to efficiently discover and pursue cybercriminals engaged in digital fraud targeting citizens of both countries. Moreover, governments and non-governmental organizations want to interact in powerful verbal exchange and collaboration on the neighborhood degree to raise public awareness approximately preventing fraud and responding to fraudulent sports. Initiating academic campaigns in colleges to inform youngsters about fraud prevention is an crucial initial step on this attempt. It is essential to cautiously bear in mind and formulate the important felony

frameworks to facilitate these measures inside the future. Emphasizing the positive conduct management of people as the key to preventing fraud is crucial. Therefore, a comprehensive expertise and application of digital criminal requirements is important for shielding structures against electronic fraud. Initial steps should additionally involve instructing the community, stakeholders, builders, and practitioners within the digital economy subject, both domestically and globally. Furthermore, endured curriculum development in this region is essential to combat electronic fraud inside each societies. (Brown & Marsden, 2023)

1.8. 8. Conclusion and Recommendations

This research has attempted to explore comprehensively the strengths and weaknesses of the current Jordanian legislation and Spanish legislation. The study found disparities in some aspects between them, which are expected, as they belong to different legal cultures and legal systems. Nevertheless, both share common denominators when attempting to fight electronic fraud adequately. The importance of each national legal framework to effectively combat electronic fraud as well as cybercrime in general is debatable but cannot be ignored. There is no one-size-fits-all solution around the world. Therefore, periodic assessment of the situation is important to highlight weaknesses, even despite the challenges that authors may face from partisans, and improve the law. (Halalsheh et al., 2021)

This study aims to promote the use of legal systems by stakeholders in both Jordan and Spain. Although there are skeptics who claim that cultural and legal differences between the two countries can create barriers, the author argues that the implementation of cost-effective plans and strategies is important to combat electronic fraud due to the inherent nature of electronic fraud. This is particularly important in a regional context to prevent cyber jihadist and terrorist activities.

As a result, several steps have been recommended to deal with electronic fraud, including: (Chhabra and Prabhakaran2023)

1. To promote cooperation and coordination between different agencies and jurisdictions with different priorities.
2. Advocate for the allocation of national and international resources to legislate and enforce cyber fraud.
3. To improve the law by integrating innovations that improve the effectiveness and efficiency of the code to promote transparency and accountability.
4. Provide regular training to staff to understand the complexities of fraud, including IT, language and electronic investments. 5. To require regulatory bodies to proactively identify and reduce the impact of electronic fraud attacks.
5. To encourage public-private partnerships to raise awareness of the risks of electronic fraud and protect investments and assets.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 12, 2025, pp. 20-33
ISSN 3104-8900

In summary, international cooperation and collaboration is successful in facilitating joint efforts to combat electronic fraud by circumventing potential interference from global initiatives. Jordanian and Spanish parliamentarians and professionals should carefully consider incorporating insights from each other's legal frameworks to improve their own legislative landscape. Periodic re-evaluation and improvement of laws is necessary to better deal with the various tactics of electronic fraud and quickly catch cybercriminals. More robust measures to police and prosecute electronic fraud in these different national contexts could discourage Internet criminals who believe that their crimes will go unpunished. (Seetharama).

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: "This research received no external funding".

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Shulzhenko, N., & Romashkin, S. (2020). Internet fraud and transnational organized crime. *Juridical Tribune*. https://tribunajuridica.eu

[2] Al-Qaaida, M. S. S. (2021). Establishing effective legal framework for new generation: A comparison of the Jordanian and some European constitutions. https://pte.hu

[3] Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-fraud in Nigerian banks: Why and how? *Journal of Financial Risk Management, 9*(3), 211–228. https://scirp.org

[4] Tambe Ebot, A. C., Siponen, M., & Topalli, V. (2024). Towards a cybercontextual transmission model for online scamming. *European Journal of Information Systems, 33*(4), 571–596. https://jyu.fi

[5] Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., & Mare, S. (2021). "We even borrowed money from our neighbor": Understanding mobile-based frauds through victims' experiences. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1), 1–30.

[6] Malik, A. A., Asad, M., & Azeem, W. (2022). The frauds in banking and entrepreneurs by electronic devices and combating using software and employment of demilitarized zone in the networks. *International Journal for Electronic Crime Investigation, 6*(4), 5–12.

[7] Stapleton, A. H. (2022). The financial fraud epidemic and how it has changed business fraud.

[8] Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*.

[9] Khater, M. N., Issa, H. A., Alsheyab, M. S., & Alwerikat, N. (2024). The crime of goods fraud in the Jordanian penal code. *Multidisciplinary Reviews, 7*(2), Article 2024035.

[10] Nukusheva, A., Zhamiyeva, R., Shestak, V., & Rustembekova, D. (2022). RETRACTED ARTICLE: Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. *Security Journal, 35*(3), 893–912.

[11] Jalghoum, Y., Tahtamouni, A., Khasawneh, S., & Al-Madadha, A. (2021). Challenges to healthcare information systems development: The case of Jordan. *International Journal of Healthcare Management, 14*(2), 447–455.

[12] Volobuieva, O., Leheza, Y., Pervii, V., Plokhuta, Y., & Pichko, R. (2023). Criminal and administrative legal characteristics of offenses in the field of countering drug trafficking: Insights from Ukraine. *Yustisia.*

[13] Saghir, W., & Kafteranis, D. (2022). The applicable law on digital fraud. In *Finance, law, and the crisis of COVID-19: An interdisciplinary perspective* (pp. 221–235). Springer.

[14] Baechler, S. (2020). Document fraud: Will your identity be secure in the twenty-first century? *European Journal on Criminal Policy and Research.*

[15] Оразхан, А. В., & Татаринов, D. V. (2020). National legislation of foreign countries on cybercrime. *Meridian Scientific Electronic Journal,* (9), 382–384.

[16] Toubat, H. S., Halim, R., & Magableh, N. (2020). The impact of technological development on legal rules: A case study of Jordan. *Journal of Critical Reviews.*

[17] Chaves-Avila, R., & Gallego-Bono, J. R. (2020). Transformative policies for the social and solidarity economy: The new generation of public policies fostering the social economy in order to achieve sustainable development. *Sustainability.*

[18] Madi, H., & Malhas, F. (2024). Applying FIDIC contracts in Jordan. In *FIDIC Contracts in Africa and the Middle East.*

[19] Abu Sarhan, T. M., & Fouché, A. (n.d.). Child sexual grooming: Listening to victims in Jordan. SSRN. https://ssrn.com

[20] Svensson-Hoglund, S., Richter, J. L., Maitre-Ekern, E., Russell, J. D., Pihlajarinne, T., & Dalhammar, C. (2021). Barriers, enablers and market governance: A review of the policy landscape for repair of consumer electronics in the EU and the US. *Journal of Cleaner Production, 288,* 125488.

[21] Triviño, R., Franco-Crespo, A., & Ochoa-Urrego, R. L. (2020). Network neutrality: The case of five South American countries. In *XV Multidisciplinary International Congress on Science and Technology* (pp. 150–161). Springer.

[22] Brown, I., & Marsden, C. T. (2023). Regulating code: Good governance and better regulation in the information age.

[23] Halalsheh, M., Kassab, G., & Shatanawi, K. (2021). Impact of legislation on olive mill wastewater management: Jordan as a case study. *Water Policy.*

[24] Chhabra Roy, N., & Prabhakaran, S. (2023). Internal-led cyber frauds in Indian banks: An effective machine-learning–based defense system for fraud detection, prioritization, and prevention. *Aslib Journal of Information Management, 75*(2), 246–296.

[25] Seetharama, Y. D. (n.d.). Architecting fraud resilience: A multidimensional strategy. Academia.edu.