Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (205-216)

Criminalizing Impersonation via Social Media Platforms

Barjes Khalil Ahmad Al-Shawabkeh[1]

Abstract

Through the use of social media platforms, this study seeks to shed light on the legal definition of impersonation, its history, the rationale behind its criminalization, the strategy employed by the criminal justice system to address it, and how unique this offense is in comparison to other similar ones. To ascertain the extent and boundaries of criminalization under the new Jordanian Cybercrime Act, the researcher used a descriptive and analytical technique to present the criminal law text of impersonation and analyze its content. This research discovered that Jordanian Cybercrime Act No. 17 of 2023 was exceptional in that it rendered impersonation on social media platforms illegal. However, because the primary characteristic of this offense's structure is its technological nature, it has proven challenging to define the boundaries and content of the offense, as well as the fact that impersonation in its new form is distinct from fraud, invasion of privacy, overstepping privacy, and illegal access. The study concludes by recommending that the minimum and maximum limits of the monetary penalty be lowered. It also highlights the necessity for the Jordanian legislature to outlaw impersonation under the Penal Code because it can be committed in real life by common means.

Keywords: Electronic Defamation (e-defamation), Cyber Forgery, Fictitious Accounts / Fake Accounts., Electronic Fraud (e-fraud), Cybercrimes.

Introduction

The rapid development of information technology and the widespread and continuous dissemination of social media platforms have led to the expansion and development of cybercrime on the one hand and the ease and gravity of the commission of cybercrime on the other (Al-Shawabkeh,2021). The practice of some disgraceful acts has increased on social media platforms, the most notable of which is the impersonation of users of such platforms, through a person creating an account, web page, group, channel, or the like on social media platforms and falsely attributing it to another person, which requires confronting this offense with criminalization. (Reasons for Jordanian Cybercrime Act).

[1] The author is a Doctoral in Criminal Law and is an Assistant Professor at Irbid National University, Irbid- Jordan. He can be reached at b.alshawabkeh@inu.edu.jo. His Orcid: https://orcid.org/0000-0001-6831-8929

The truth is that at the penal level, the legislative system was not devoid of provisions criminalizing the offense of impersonation in general, whereas Article (417/1/C) of the traditional provisions of the Jordanian Penal Code No. (16) of (1960) provides for the indirect criminalization of this act, considering impersonation as a means of fraud, and it is punishable as follows: "Anyone who induces another person to hand over to him movable or immovable property or documents containing an undertaking or acquittal and then taking it over fraudulently: (c) By using a false name or an incorrect characteristic."

The fraudulent offender may take a false name to induce others to extradite their money to seize it, but this does not apply to someone who takes a false name or an incorrect characteristic as an independent incident, because the offense of fraud falls within the penal protection of funds without persons. Accordingly, Article (417) of the Penal Code failed to criminalize impersonation, and this provision applies to Article (10) of the new Cybercrime Act No. (17) Of (2023), criminalizes cybercrimes based on electronic fraud (e-fraud).

Other attempts to criminalize impersonation under Penal Code No. (16) of (1960), Article (202) of the Code penalizes the following: "Anyone who impersonates a civil or military public servant in event that official servant is assigned to carry out an act or attend a place ex officio, or (b) Unduly pretended to be a civil or military public servant and claims that he has the right to perform any act or attend a place to perform any act ex officio." Article (213) of the same Act also criminalizes: "Whoever assumes the name of another in a judicial investigation or trial."

Although the Penal Code attempted to criminalize impersonation in the text of Article (202), this was not possible because this provision mentioned it solely as an offense against the public authority, as is the case in the provision of Article (213), according to which the legislator stipulated that the impersonation to only be during Trial procedures as an offense against the justice conduct.

The provisions of the Penal Code failed to criminalize impersonation, due to the technical progress, technological development, and digital interactions among individuals, which led the Jordanian Penal legislator to criminalize this act by promulgating the Provisional Information System Offenses Act No. (30) Of (2010), where Article (3) of the Act criminalized intentional access to any website or information system without a permit, or to violate or exceed the permitted limit to impersonate the identity or personality of its owner.

Article (3/b) of the Provisional Information System Offenses Act requires illegal access to the website, the place of fraud, for the offense of impersonation to occur, but what if the site was accessed legitimately and its owner identity or

personality was impersonated, as legitimate access to the website, does not prevent impersonation of its owner?

These dilemmas were addressed by promulgating the Cybercrime Act No. (27) in (2015), replacing the Information Systems Offenses Act. Article (3/c) of the (2015) Act criminalizes intentional access to any website to impersonate the identity or personality of its owner regardless of whether such access is legitimate.

Despite the solution to the above-mentioned dilemmas, another, more serious dilemma remains, when envisaging the possibility of impersonating any person without having to access his website or information system at all, by creating a page, website, or electronic account bearing that person's photograph, his name or any data concerning his identity, and therefore Article (3/c) of the Cybercrime Act No. (27) Of (2015) remains unable to criminalize impersonation in this sense, which led the Jordanian legislator to promulgate a new cybercrime Act of (2023).

Literature review

The following section provides the latest studies related to criminalizing impersonation via social media platforms. Here are some of the studies.

The Study of Al-Qarala, (2023) Physician Impersonation in Medical Professions aimed to clarify the terminology related to the offense of the impersonation of a physician, finding a doctrinal adaptation, and reviewing its punishments. The study concluded, among other things, that the legal punishment for impersonating a physician is through doctrinal adaptation (Chastisement), which is what the imam deems appropriate to reach the deterrent punishment. The punishment is varied among jurists, while in Jordanian law the penalty is limited to imprisonment and a financial fine.

Al-Ajmi (2022) did a study on the Offense of Impersonation on Social Media Sites. This study addressed the definitions governing the offense of impersonation in social media as a fraudulent offense and clarified legitimate judgment (Sharia) and Kuwait's legal position in terms of criminalization and punishment. The study concluded that the offense includes several forbidding and legitimate criminalization, and thus includes it under penalties. The offense is also based on a physical element, represented by impersonating a false name or assuming an incorrect capacity, and a moral element, represented by the presence of the elements of knowledge and will, as Kuwaiti law punishes this offense with imprisonment and a fine.

The Study of Baazizi (2023) The Offense of Impersonation in Islamic Law (Sharia) and Algerian Law, examined the concept of the offense of impersonation, its elements, methods of commission, and penalties. This study found that impersonation is an essential element in its criminalization, in addition to its

physical and moral elements. Accordingly, Algerian law prescribes penalties for this offense, including imprisonment, fines, and both.

Menkhervis (2023) studied cybercrimes via Social Media Sites with Social and Ethical Dimensions. This study dealt with the most prominent cybercrime via social media sites that are influenced by the social and moral circumstances of society and its transformations. This study found that this type of offense is the most widespread among members of society, as its users took an illegal path in exploiting it, which led to offenses that affected the honor of individuals, such as insult, slander, defamation, impersonation, and exploitation of minors.

The Importance of the Study

Because the legislator is most familiar with the circumstances of his environment, he enacts penal texts as required by the reality of the situation to maintain the security system and societal peace, especially in light of the development of communication between individuals and the spread of social media sites that allow them to communicate with each other without time or geographical restrictions. Current Cybercrime Act, no. (17) Of (2023) was issued, which replaced Cybercrime Act No. (27) Of (2015), the new law provided a unique text that criminalizes impersonation via social media platforms in particular.

Impersonation has become an offense under Article (5) of the new Cybercrime Act No. (17) of (2023), it is necessary to study the criminalization of impersonation via social media platforms, separately from the offenses of violating privacy and assaulting individuals' privacy, bearing in mind that some Western legislation calls this offense "electronic identity theft," including the US Impersonation Act (1998), which criminalized this act as a federal offense.

Objectives of the Study

This study responds to the research questions raised in the pursuit of a set of objectives as follows:

- Demonstrate the notion of impersonation and the basis for its criminalization in the updated form.
- Attempting to detect and identify the acts that constitute an offense of impersonation and determine their means.
- Highlight the features of the Cybercrime Act in confronting and combating acts of impersonation.

Study Questions

This study, titled (Criminalizing Impersonation via Social Media Platforms), was launched from a broad question that was raised due to the new legal structure for this offense, by which the Jordanian legislator was singled out in Article (5) of the Cybercrime Act of (2023), which raised the following questions:

• What is the notion of impersonation as a new offense independent of the offenses of violating privacy and assaulting individuals' privacy?

• What is the basis for criminalizing impersonation as it is physically permissible if it is not done by electronic means?

• What is the Jordanian legislator's plan to confront impersonation and criminalize it?

Method

Fulfilling the purpose of studying the criminalization of impersonation via social media platforms, the researcher followed the descriptive approach of presenting the criminalized legal texts of impersonation and describing its content to distinguish this offense from other similar offenses such as cybercrime, espionage offenses, and illegal technical entry. The researcher also followed the analytical approach in this study to analyze the terms of the criminal text of impersonation, determine the scope of this crime, indicate its limits and the basis for its criminalization under Jordan's new Cybercrime Law No. 17 of 2023, and read some of its judicial applications that criminalized impersonation via social media platforms.

Results and analysis

The notion of impersonation across social media platforms as a new offense is confined to creating a social media platform through cyberspace and falsely attributing it to a natural or legal person.

Article (5/A) of the Cybercrime Act No. (17) of (2023) criminalized impersonation via social media platforms in a specific and distinct way that differs from the forms of criminalizing impersonation previously addressed by the Jordanian penal legislator, where there is no longer room for debate about impersonation as a means of fraud as a composite offense, whether traditional contrary to the provisions of Article (417) of the Penal Code (Ersan, 1990) or electronic contrary to the provisions of Article (10) of the Cybercrime Act (soulmeen, 2009).

A new offense (impersonation via social media platforms) does not require illegal access to websites or social media platforms, as it is possible for the offender

to commit this offense without the need to create a social media platform and attribute it to a natural or legal person.

The criminalization of impersonation is no longer coupled with infringement of privacy or assaulting the private lives of individuals, such as impersonation before the issuance of Article (5/A) of the Cybercrime Act No. (17) Of (2023) was merely one of the elements of the offense of prohibited access or its ultimate purpose. The Jordanian legislator did as well (Abiyah, 2021).

The offense of impersonation may occur through websites or social media platforms without the need to access (legally or illegally) the websites or social media platforms of the victims of fraud because impersonating the user does not require access to his/her programs or social media platforms (Tala, 2020).

Using Social Media Platforms as a Basis for Criminalizing Impersonation

The new Jordanian Cybercrime Act is unique in that it criminalizes impersonation through social media platforms, as the use of social media platforms has become the basis for criminalizing impersonation (Abdallah, 2021). The Jordanian Penal Code did not address the offense of impersonation in the abstract and assumed that the offense existed in the case of impersonating an official as part of a public authority offense or while impersonating a person during procedures as an offense against the course of justice. So long as all the necessary components and aspects of the conduct are present, impersonating someone's identity is not illegal unless it is done through social media platforms or by inventing, building, or designing a software, application, website, email, or anything else similar (Al-Shawabkeh، 2024).

Social networking platforms are social networks on the Internet, allowing communication between their users in a virtual community environment that brings them together according to their social and cultural interests or affiliations. This is done through direct communication, such as sending messages, photos, videos, audio clips, etc. The participation of others and knowledge of their news make participation in these platforms easy and accessible as the individual becomes a user of these platforms that open the world to him (Fahmi, 2017).

Cybercrime Act No. (17) Of (2023) Art. (2) Social media platforms are defined as any electronic space that enables users to create an account, page, group, channel, etc., through which the user publishes, sends, or receives images, video clips, comments, writing, numbers, symbols, or audio recordings. "Facebook, Instagram, LinkedIn, Snapchat, TikTok, and WhatsApp" are among the most well-known platforms. It is important to remember that social media platforms are uncontrollable, owing to their constant invention and development.

Social media platforms are effective tools that allow people in society to interact, entertain, share news and their perspectives, and voice their thoughts on a wide range of topics including politics, the economy, society, culture, education, and other facets of daily life. According to Dababneh (2015), these platforms dominate the usage and dissemination of electronic media; the more a medium is utilized, the more widely it is used, and vice versa.

Because "websites" contain "social media platforms," which are regarded as a component of the former, the previous Cybercrime Act did not include social media platforms as a means of committing informational crime. However, the updated Cybercrime Act of 2023 recognized the seriousness of using social media platforms to perpetrate impersonation crimes and specifically included it as a method of doing so and a component in the creation of the law.

Although the criminal legislator did not consider the methods of criminalization as a general principle (Majali,2022), social media platforms are among the technological means used to perpetrate the offense of impersonation. Regardless of how crimes are committed, they are still illegal. However, the Jordanian penal legislator has made an exception to this rule for previously stated reasons and goals, such as the ease with which cybercrime related to social media platforms can be committed, the difficulty of establishing it, and the seriousness of its consequences (Al-Shawabkeh 2020).

The Cybercrime Act's Features in Addressing and Preventing Acts of Impersonation

The features of the Cybercrime Act in confronting and combating acts of impersonation are evident by not specifying the nature of the acts of impersonation via social media platforms by strictly punishing the offense of impersonation by imposing a high fine.

Failure to Specify the Nature of Impersonation Acts via Social Media Platforms

Creating an account, web page, group, channel, or similar social media platform is not enough to commit the offense of impersonation; rather, it must be attributed falsely to a natural or legal person. False attribution refers to attributing the social media platform to the victim by writing his/her name, surname, or any data indicating his/her personality, or by placing his/her picture on this platform, for the users to understand that this account or platform belongs to the victim.

The Jordanian legislature does not specify the nature of the content or the type of data that the offender must falsely attribute to the victim via the social media platform to impersonate him, as it is sufficient that this content or data is a

conclusive indication of the identity of the victim and not of any other person. Hence, the legislator did not specify the nature of acts of impersonation through social media platforms because cybercrime is technical (Sahafi, 2020), and the legislator cannot limit its scope and predict what will be developed technically in the future (Al-Zubaidi, 2018).

The Madaba Magistrates' Court found the defendant guilty of impersonation via social media platforms in the incident: “Creating a fake page on the Instagram and Facebook applications under the name of the complainant... From that page, communication was made with her students and friends, her pictures were uploaded to that account, and inappropriate verbal overtones were made in the name of the complainant.” (West Amman Penal Magistrate Ruling, No. 2466/2022).

Al-Salt Magistrate's Court also convicted the defendant of the same offense in the incident: “The accused visited the complainant in her clinic where she works as a dentist, and after that, the dentist heard that there was an advertisement on the Snapchat application by her name and address that she performs breast augmentation surgeries, and address that she conducts breast augmentation surgeries and those who wish to contact her for early detection. The complainant did not file any complaint at that time, but after that, a person from another account contacted the complainant on her Instagram account, asking her to book an appointment at the clinic. It turned out that that account was impersonating her name and with the same content as the breast augmentation advertisement, and it later became clear to her that the owner of this account was the accused." (Al-Salt Penal Magistrate Ruling, No. 2439/2023).

The researcher observed, through the judicial application of Article (5) of the Cybercrime Act on some offenses of impersonation via social media platforms, that the manner and means of committing the offense differ depending on the person, the circumstances of the offense, the nature of their work, the type of social media platform they use, and the objectives that perpetrators aspire to shape through impersonation, although the motive for the offense is irrelevant (Penal Code, Art. 67).

Aggravating the Penalty for the Offense of Impersonation by Imposing a High Fine

A person may not be held criminally liable unless the offense is accompanied by a penalty. By referring to the provisions of Article (5/A) of the Cybercrime Act, it is observed that the legislator has punished the offense of impersonation with imprisonment for no less than three months or a fine of no less than 1,500 JD. One thousand five hundred dinars, and not more than 15,000 JD. Fifteen thousand dinars, or both of these penalties.

It is noted that this punishment includes two types of punishment: the first type is a custodial penalty, which is imprisonment for a minimum period of three months and increases to a maximum of three years according to the general rules as a misdemeanor punishment (Penal Code, Art. 20), while the second type is the financial punishment, which is represented by a fine to be paid by the convict in an amount not less than one thousand five hundred dinars and not more than fifteen thousand dinars, with the possibility of doubling the application of these two penalties together.

Through the aforementioned fine, the researcher observes that the Jordanian legislator granted the criminal judiciary broad jurisdiction to determine the financial penalty for the offense of impersonation, with a maximum amount of fifteen thousand dinars, or roughly twenty-one thousand US dollars (21,000). Based on the current state of affairs and economic conditions in the Jordanian state, this penalty is extremely severe and severely affects anyone who attempts to pose as someone else.

As the fines from the convicted go back into the public coffers, this is not meant to be punishment in the traditional sense, nor is it meant to be payback or revenge against people. By imposing the financial penalty, the lawmaker hopes to establish a criminal code that addresses the danger that individuals pose to the entity and discourages those who would try to pass for someone else to uphold and safeguard their reputation.

The legislator was correct to include a financial charge in his punitive proposal, with a maximum amount that might be fifteen thousand dinars. These kinds of fines are now the standard in criminal policy to dissuade offenders (Wreikat, 2013). The Jordanian lawmaker is also criticized for giving the criminal court discretion over how much of a financial fine to impose, with a wide disparity between the minimum and maximum limitations.

Conclusion

A study of impersonation via social media platforms revealed the ambiguity of the legal structure of this offense and the Jordanian legislator's penal policy to combat and confront this offense, especially since this offense, with the promulgation of the new Cybercrime Act of 2023, was separated from other fraud offenses, violations of privacy, assaults on individuals' private lives, and illegal electronic access.

The Jordanian legislator restricted the notion of impersonation via social media platforms as an innovative offense on the creation of social media platforms via cyberspace and falsely attributed it to a natural or legal person. The legislator limited the criminalization of impersonation using social media platforms and did

not specify the nature of acts of impersonation given the ongoing development of social media platforms, their tools, and software, which are the cyberspace for this offense. The legislator also increased the penalty by imposing a high fine on the perpetrators of this offense as an active penal policy for acts of impersonation and combating them.

Recommendations

Since the Penal Code is the guarantor of security, community peace, and penal protection for persons without Assault on their entity in any way, the criminal text of impersonation must be capable of confronting this crime in a highly effective manner to ensure that persons are protected from the crime of impersonation of all persons. Her images and patterns, so the researcher's study of the crime of impersonation concluded through social media platforms. The state party refers to the Jordanian Penal Code's legal recommendations as follows:

- Some minor amendments to the text of Article 5 of the Electronic Crimes Act No. 17 of 2023. The most important of these is to reduce the difference between the minimum and the highest levels of the fine without the release of an authority.
- The judiciary's judgment. The Jordanian legislature criminalizes impersonation under the provisions of the Penal Code for the possibility of committing such an act. The crime is realistic or material by using ordinary means away from social media platforms or other electronic means.
- Criminalizing the attempted crime of impersonation through social media platforms despite the difficulty; Preventive criminalization and proactive penal liability provide preventive security for users of media platforms. Social, by sowing awe with punishment in the same person who begs his foot on this crime even if Its result has not been achieved.

References

Abdallah, A. (2021). Public Office Impersonation and Scope of Responsibility. *Journal of Law, Faculty of Law, University of Montassiria*, 13 (41), 149 - 170.

Abiyah, K. (2021). The Legislative Template for Electronic Impersonation Offense and Identity Theft: A Comparative Study, *Journal of Humanities and Administrative Sciences, Majmaiyah University*, Issue (22), 87-112.

Al-Ajmi, M. (2022). The Crime of Catfishing on Social Media Comparative Islamic Jurisprudential Study With Kuwaiti Law, *Journal of Sharia and Islamic Studies,* 37 (130), 174-219.

Al-Qarala, R. (2023). Physician Impersonation in Medical Professions: A Jurisprudential Study Compared to the Jordanian Penal Code. *Al-Mizan Journal of Islamic and Legal Studies, International Islamic Sciences University,* 10 (13), 13-36.

Al-Shawabkeh, B. (2020). Common Cybercrimes on Social Networking Sites. *Journal of Studies, Amar Telidiji University*, 91, 137-152.

Al-Shawabkeh, B. (2021). Criminal Confrontation of Fake News and Fabricated Facts in Light of the Corona Pandemic. *First International Youth Researchers' Forum, Publications of the Faculty of Legal Sciences at Ibn Zahr University, Kingdom of Morocco, Series of Collective Literature*, 3, 267-288.

Al-Shawabkeh, B. (2024). Criminalization of Personality Assassination Via Electronic Means. *Journal of Law and Sustainable Development, Miami*, 12(1), 01-20.

Al-Zubaidi, D. (2018). Offence of Assault on Websites. *Babylon University Journal*, 26 (9), 392-408.

Baazizi, S. (2023). *The Offense of Impersonation in Islamic Law (Sharia) and Algerian Law - Master's Thesis*.Ahmed Draya University, Edrar - Algeria.

Cybercrime Act No. (17) Of (2023).

Cybercrime Act No. (27) Of (2015).

Dababneh, Sh. (2015). Cybercrime - Electronic piracy. *Journal of Financial and Banking Studies, Arab Academy of Financial and Banking Sciences, Centre for Financial and Banking Research*, 23 (1), 22-19.

Ersan, A. (1990). fraud: impersonation is an offense that results in other crimes such as monument Tzui, Security, and Life. *Naif Arab University of Security Sciences*, 9 (111), 53-57.

Fahmy, D. (2017). *Criminal liability arising from the use of social media sites*, search provided Fourth Scientific Conference of the Faculty of Law at Tanta University entitled Law Media.

Jordanian Penal Code No. (16) Of (1960).

Judgment No. (2439 of 2023) - Al-Salt Penal Magistrate Court, issued on (25/10/2023). Jordanian Bar Association

Judgment No. (2466 of 2022). West Amman Penal Magistrate Court, issued on (19/12/2023). Jordanian Bar Association

Majali, N. (2022). Explanation of the Penal Code General Section. *Jordan, Culture Publishing and Distribution House*, p. 8.

Menkhervis, Y (2023). Cybercrimes via Social Media Sites with Social and Ethical Dimensions. *Journal of Law and Human Sciences*, Zian Ashour University at Jelfah, 16 (1), 1313-129.

Reasons for the draft Jordanian Cybercrime Act (H.A -09-07-2023).

Sahafi, R (2020). *Cybercrime, Global Multidisciplinary Electronic Journal*, 24 (5), 1-53.

Swelmeen, I. (2009). Fraud Crime through the Internet: Comparative study between the Jordanian and the Egyptian Law. *Graduate School of Law Amman Arab University*, 1-220.

Tala, L. (2020). Cyber Crime: A New Dimension to the Concept of Crime across Social Media Platforms. Hallway Journal of Social and Human Studies, Ahmed Zabanah University Centre. Glezan Informant *for Social, Psychological and Anthropological Studies*, 6 (2), 62-91.

The Provisional Information System Offenses Act No. (30) Of (2010).

Wreikat M. (2013). The validity of a fine as an alternative to short-term imprisonment in Jordanian and comparative legislation. *Al-Najah University Journal of Research (Human Sciences)*, 27 (5).