Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (1287-1298)

The Problem of Jurisdictional Conflict and the Applicable Law on Cybercrime

Hassan Yousef Magableh[1],
Barjes Khalil Ahmad Al-Shawabkeh[2]

Abstract

This study addresses the issue of jurisdictional conflict and the applicable law on cybercrime, which has had a clear impact on criminalization and punishment. In addition, the procedural aspects of combating these crimes that transcend borders, pose many challenges in terms of jurisdiction, especially given the differences in legislative frameworks and the weakness of international cooperation in this field. The study initially focuses on explaining the legal nature of jurisdictional conflicts and their impact on cybercrime. It also highlights the issues related to the perpetrator's multiple nationalities. The study concludes that jurisdictional conflict arises from states' adherence to the principle of sovereignty over their territories and people, and the absence of unified legislation to resolve disputes over the applicable law. The study exceptionally suggests applying the principle of personal jurisdiction with an affirmative approach and the principle of universal jurisdiction under specific conditions. The study recommends amending Article (7) of the provisions of the Penal Code and Article (38) of the Cybercrime Law in Jordan to include the principle of regional jurisdiction for attempted cybercrimes committed abroad and where the criminal result is not achieved within the Jordanian territory.

Keywords: little arrow, information technology, except empowerment, personal affirmation, self-validity.

Introduction

The recent decades have witnessed a tremendous revolution in the field of technology and communications, which led to the emergence of new remote communication methods that have reshaped the world, making it a small global village without borders. These technologies have been used in various aspects of life within countries at all levels, especially after the development of information systems and their connection to satellites (Khansaa, 2010).

Despite the enormous benefits brought about by information technology across various areas of modern life, this growing technological revolution has

[1] Associate professor – law department, Irbid National University. h.magableh@inu.edu.com ORCID: https://orcid.org/0009-0000-9474-6169
[2] Assistant professor, Irbid National University. b.alshwabkeh@inu.edu.jo ORCID : https://orcid.org/0000-0001-6831-8929

been accompanied by a range of serious negative consequences due to the misuse of advanced technologies and deviating from their intended purposes. One of the emerging criminal phenomena resulting from this technological revolution is the phenomenon of cybersecurity crimes. These risks have escalated, particularly in the virtual environment represented by the widespread international information network (the Internet), and their dangers are no longer confined to the regional scope of a particular country (Shayen, 2022).

Cybersecurity crimes are characterized by their difficulty in detection and proof since they involve hidden attacks that operate outside the tangible physical realm. Multiple perpetrators often collaborate in committing these crimes, possessing technical skills in the fields of computers and information security that enable them to engage in hacking, sabotage, espionage, or the decryption and cracking of software codes. These crimes transcend borders, as there are no longer concrete or visible boundaries hindering the transfer of information between countries. Due to the capacity of computers and their networks to transmit vast amounts of data, multiple locations in different countries may be affected by a cyber-attack, with the perpetrators in one country and the attack occurring in another. This situation poses various legal and operational challenges to law enforcement agencies, particularly concerning the issue of jurisdictional conflicts and the applicable law in cases of cybercrime.

The technical revolution has created a new world, the cyber world, which has resulted in many advantages for individuals, but some of them have negatively exploited it to commit criminal acts, which have been characterized by crimes that have no borders. The perpetrator may reside in one country and the victim in another. This impedes the completion of investigation and trial proceedings, especially as cyberattacks increase globally. (29%), as actors continue to exploit these problems in their crimes and global damage increases, with global losses projected annually to rise to $10.5 trillion.

Study Problem

The escalation of cybercrimes, committed through cyberspace, has negative implications for the criminal justice system. Perpetrators of these crimes easily exploit cyberspaces, considering them their haven, especially since these crimes transcend borders. This presents an objective and procedural problem due to the multiplicity of laws applicable to cybercrimes. The wide-reaching consequences and damages of cybercrimes give rise to challenges related to the perpetrators themselves. Questions arise about whether the perpetrator possesses multiple nationalities or is stateless while committing these crimes. The criminal may commit the offense in one country that criminalizes their actions within its jurisdiction, but because they hold citizenship in another country, they may also be

subject to punishment under the principle of personal jurisdiction. Additionally, there is a primary challenge regarding conflicts between international laws in applying legislation to cybercrimes.

Research Questions:

From this primary problem, several sub-questions emerge:

1. What is the legal nature of jurisdictional conflicts, and how does it impact cybercrime?
2. What are the obstacles related to the perpetrator's multiple nationalities or statelessness concerning cybercrimes?
3. Which law should be applied if these attacks are carried out by one country against another?

Study Objectives

The study of the issue of conflict of jurisdiction and the law applicable to cybercrime answers the research questions posed so that this study seeks to achieve a set of objectives as follows:

1. Clarify the legal nature of jurisdictional conflicts and the impact of legal conflicts on cybercrime.
2. Shed light on the issues related to the perpetrator's multiple nationalities or statelessness concerning cybercrimes.
3. Identify the applicable law when such attacks are committed by one state against another.

Methodology

The study adopts an analytical and descriptive method by referring to legislative texts represented by national laws and international agreements. These sources were chosen in particular because they address the issues of jurisdictional conflicts and the applicable law for cybercrimes. Additionally, the study will discuss some jurisprudential opinions on these matters.

Data Analysis

Section 1: Issues Related to the Multiplicity of Laws Applicable to Cybercrime

The complexities related to the multiplicity of laws applicable to cybercrime stem from various motivations and reasons, with the foremost being the respect for a state's authority and sovereignty within its territory. This principle is known as the territoriality of the legal rule and emphasizes a state's power to hold its citizens accountable for committing crimes stipulated by law, particularly in the realm of criminal law (Nassif, 2016).

Subsection 1: The legal nature of the conflict of laws

Article (29/1) of the Arab Convention on Combating Technology Offences obligates each of the contracting states to enact the necessary legislation and procedures concerning the crimes stipulated in their domestic law. Therefore, it is natural for various legislations to have been enacted to address cybercrimes or information crimes (Al-Saiedi, 2010). This is under the principles of criminal law, such as the principle of personal jurisdiction and the principle of territorial jurisdiction in the application of a state's criminal law to crimes that occur within its territory, or when one or both parties hold its nationality, leading to conflicts over the application of the state's law to this crime (Jaber, 2007). The legislative variations among countries not only affect the substantive rules of the law but also extend to the procedural rules concerning prosecution, investigation, and inquiry (Khalifa, 2016).

Some aspects of jurisprudence argue that such conflicts lead to a lack of clarity regarding the jurisdiction of both the judiciary in handling these crimes on the one hand and the applicable law on the other hand. In other words, the cybercriminal commits a crime characterized as transnational, passing through information networks and digital systems either within or outside the state or within the state's systems (Al-Shawabkeh, 2004).

Another aspect of jurisprudence argues that raising the issue of conflicts of laws is related to considerations concerning state sovereignty. If the perpetrator holds the nationality of the judge's state, personal jurisdiction is applied according to the judge's nationality law, not the foreign law, unless the perpetrator's nationality differs from that of the judge in a manner that does not raise conflicts of laws (Abdul Qadir, 2022).

It can be argued here that the foundation of the concept of conflict of laws is built on the principle of a state's sovereignty over its territory and its people. The adherence to this principle and the absence of international cooperation in responding to all arising cybercrimes and their systems with a unified law make the process of reconciling the applicable laws a complex and debated issue in its determination and designation. This, in turn, affects the detection of the crime, the acquisition of evidence, and the tracking and prosecution of cybercriminals.

Subsection 2: The impact of the conflict of laws on cybercrime

The divergence of applicable laws has led to the creation of numerous national and international alternatives for resolving various types of disputes. Because of this divergence, countries have entered into various types of treaties, agreements, and memoranda concerning any incident that may occur in the future (Al-Jubouri, 2020).

Furthermore, the raising of conflicts of laws and their inadequacy at the same time has compelled countries to enact legislation and laws specifically addressing cybercrimes. This involves the development of the digital infrastructure and the engagement of experts and specialists in establishing the legal and technical frameworks for addressing them both legally and procedurally.

Following the introduction of these legislations, another issue arose on a different level. Nationally, problems related to the application of two or more national laws to a single criminal incident emerged. This is known as the moral plurality of the crime, where the criminal act is the same, but different legal descriptions and behaviors apply to it under multiple legal provisions. An example of this is when a public employee breaches the system of the public institution they work for, stealing data about a specific citizen to manipulate information about them, such as making them appear older or issuing a false death certificate (Al-Ghata, 2012), among other similar actions. In this case, it is a situation where the conflict of domestic laws or the application of the laws of two different countries to the same criminal incident arises, and each country assigns and adheres to its national law for the application of the crime in its various aspects, both positive and negative.

Section 2: Problems relating to the perpetrator's multiple nationality or lack thereof about cybercrime

Subsection 1: Issues related to the dual nationality of the perpetrator in cybercrime

In terms of the penal aspect related to cybercrime, we find that the Jordanian legislator has included a specific provision regarding jurisdiction, through which we can determine the applicable law. For example, Article 5/4 of the Criminal Procedure Code No. 9 of 1961 states that public prosecution proceedings may be initiated in Jordan if cybercrime is committed through electronic means outside the kingdom of Jordan, and its effects occur either wholly or partially within Jordan, or if the crime affects any of its citizens. Article" 38 of the Electronic Crimes Law No. 17 of 2023 also specifies that "legal action for public and personal rights may be brought before the competent judicial authority if any of the crimes stipulated in this law are committed using information networks, information technology, information systems, social media platforms, or any online publishing medium inside or outside the kingdom of Jordan, and if the crime causes harm to Jordan's interests, its citizens, residents, or if the effects of the crime occur wholly or partially in Jordan".

In light of these legal provisions, the Jordanian legislator has established criteria for the Jordanian judiciary to have jurisdiction over cybercrimes. These criteria include the following:

1. If the cybercrime is committed within the kingdom of Jordan and is stipulated by law.
2. If the crime causes harm to Jordan's interests.
3. If the crime causes harm to residents in Jordan.
4. If the results of the crime or its effects occur wholly or partially within Jordan.
5. If the crime is committed by one of the individuals residing in Jordan.

However, it is worth noting that in this field, more than one country may claim jurisdiction over a cybercrime due to their adherence to the principles of territorial or personal jurisdiction under their national laws. This can lead to a conflict of laws regarding the applicable legal framework. What is the legal solution to this positive conflict?

We believe that the legal solution to the idea of conflicting laws lies in granting jurisdiction to the state in which the cybercriminal resides on its territory or boards a ship bearing its flag, or an aircraft registered under its laws at the time of the crime, regardless of the criminal's nationality. It involves resorting to the principle of personal jurisdiction if the individual holds that nationality. In cases where multiple states claim jurisdiction over cybercrime, the concept of consultation or applying the principle of universal jurisdiction to the state where the habitual residence of the person committing the crime can be utilized. This approach is embraced by Article 22 of the Budapest Convention on Cybercrime of 2001 and Article 30 of the Arab Convention on Combating Information Technology Crimes of 2010 (Article 30, 2010).

In this context, it is notable that the Jordanian legislator has adopted the principle of territorial jurisdiction as a fundamental principle in exercising jurisdiction over cybercrimes, whether the crime occurred entirely within the state's borders or if one of the acts constituting the material element of the cybercrime took place in it. This includes the criminal activity, the criminal result, or the causal relationship between them. This is based on Article 7 of Jordan's Penal Code No.16 (Article 7,1960), which states that “the provisions of this law apply to any individual who commits a crime within the territory of the Kingdom”, as outlined within it, in addition to that the crime is considered to have been committed in the Kingdom, “if one of the elements that constitute the crime, an act of an indivisible crime, or an act of primary or secondary association takes place on the territory of this Kingdom.”

However, it is noteworthy that the Jordanian legislator does not consider cybercrime to have occurred within Jordan's territory unless the result has occurred. The legislator excluded the notion of committing the crime abroad and expecting the criminal result to take place within Jordan's territory from the scope of the provisions of (Article 7 of the Penal Code & Article 38 of the Cybercrimes Law). The legislator also excluded attempts to commit cybercrimes committed abroad if the criminal result does not occur within Jordan's territory for reasons beyond the cybercriminal's control. The legislator also excluded cybercrimes from the scope of crimes subject to the jurisdiction of the International Criminal Court according to the principle of territorial jurisdiction, as provided by Article 9 of the Penal Code, which exclusively listed specific crimes for the application of this principle.

There is no objection to applying the principle of personal jurisdiction to all forms of cybercrimes, especially since they can be of the nature of felonies or misdemeanors, even if committed by a person holding Jordanian nationality abroad upon their return to the Kingdom. This is because the Jordanian legislator does not require dual criminalization according to this principle, even if the individual loses Jordanian nationality or acquires it after committing a cybercrime of a felony or misdemeanor. Furthermore, the principle of universal jurisdiction can be applied if the cybercriminal holds foreign nationality, and the crime is of the nature of a felony or misdemeanor, with the condition of residence on Jordanian territory.

In this regard, it is hoped that the Jordanian legislator will consider the specificity of cybercrimes and amend the criminal jurisdiction rules to include the case of attempting to commit a crime under the principle of territorial jurisdiction. This should be included among the crimes subject to personal jurisdiction, without requiring the cybercriminal's residence to be subject to the principle of universal jurisdiction, with only the condition of transit or presence.

The other question that arises in this context is whether, in cases where multiple countries claim jurisdiction over the commission of cybercrime, and especially in the absence of national laws, international legislation represented by the Budapest Convention, and regional legislation represented by the Arab Convention on Combating Technology Offences, how is this issue resolved? This occurs when each country declares its judicial competence regarding cybercrime, leading to a situation of positive conflict and applicable laws.

In this regard, criminal jurisprudence is divided into two approaches. The first approach leans towards applying the most suitable law, which is the law of the state most affected by cybercrime. Advocates of this approach consider the extent of the damages resulting from cybercrime, and the varying degrees of harm

among states to make the jurisdiction favor those states most harmed. However, critics argue that this approach is limited in addressing all cases of damage caused by cybercrime, as it may not account for situations where the harm is equal among states, leaving room for ongoing conflicts (Jamil, 2010).

The second approach adopts the principle of anticipated harm, which means that the jurisdiction should be based on the potential harm that cybercrime can cause in any state connected to the Internet. In this case, all affected states would be equally harmed, and thus, it becomes impossible to apply the law of the state where the crime occurred. Instead, the jurisdiction reverts to the law of the state in which the crime was committed (Hijazi, 2007). This principle was affirmed by the European Council for Justice when it determined that information published on the Internet can reach all connected states, regardless of whether the harm is specifically directed, and thus, the principle of anticipated harm applies to the person responsible for harmful information due to the nature of this medium (Benslimane, 2017).

Subsection 2: Issues related to statelessness of the perpetrator in cybercrime

Statelessness refers to a condition in which an individual does not possess the nationality of any specific country. A person can be in this condition if their nationality is revoked or withdrawn by their country, or in cases where there is a negative conflict among states regarding a person, and all states and their laws disclaim jurisdiction over the individual, resulting in the absence of a genuine dispute over the application of the law on them (Mahmoud, 2021).

Regarding the criminal aspect related to cybercrimes committed abroad, jurisdiction can be established based on the nationality held by the cybercriminal at the time of committing the crime, even if they later became stateless or acquired a different nationality. This is by the principle of personal jurisdiction, as stated in Article 10/1 of the Jordanian Penal Code.

In cases where statelessness continues for the cybercriminal, jurisdiction can be established based on the principle of territorial jurisdiction as outlined in Article 7/1 of the Jordanian Penal Code and Article 38 of the Cybercrimes Law. According to these laws, criminal jurisdiction applies to every resident who commits a crime within the Kingdom of Jordan, regardless of whether the perpetrator is a citizen, foreigner, or stateless person. This is subject to the provisions of immunity granted under international or national law, as per Article 11 of the Jordanian Penal Code.

In this regard, it is believed that such a situation may arise when a cybercrime is committed by a stateless person who has immigrated illegally to a specific country after having their original nationality revoked. Subsequently, they

engage in criminal activities on the Internet, such as human trafficking, drug trafficking, or sexual exploitation. In this case, the jurisdictional conflict arises due to the absence of a specific law governing the perpetrator, and the mentioned provisions regarding the application of the law of the country where they reside can be considered (Article 30, 2013).

It is worth noting that cybercrime is a borderless and transnational offense. It is conceivable that a cybercrime could be committed in one country while the perpetrator resides in another, or it could involve one country taking action against another. This situation can lead to conflicts in laws, and thus, the challenge lies in determining which law should be applied and whether the cybercrime constitutes an act of cyber warfare (Hasan, 2016).

The researcher believes that cyberattacks occurring between states have a unique legal nature governed by rules of international law related to the regulation of relations between states. These rules include obligations for states to respect the sovereignty of other states, criminalize the use of force in international relations, and prohibit any form of aggression. Furthermore, cybercrimes cannot be applied to states in a criminal sense, similar to other legal persons and natural persons. Hence, it is necessary to explore alternative adaptations.

Labeling such attacks as "cyber wars" may not be appropriate since the rules of international law require the presence of traditional armed conflict to classify these attacks as wars. In this regard, it is hoped that international lawmakers either establish a specialized court for cybercrimes or redefine the crime of aggression as stated in Article 8 bits of the Rome Statute of the International Criminal Court of 1998 to include cyberattacks launched by states against each other under these circumstances.

Conclusion

In conclusion, this research has highlighted the complexity of jurisdictional issues in cybercrime cases, both nationally and internationally. It has emphasized the need for a clear legal framework to address these challenges and ensure that cybercriminals are held accountable for their actions. The results provided in the research aim to contribute to the ongoing discussions and efforts to develop effective legal mechanisms for addressing cybercrime in the modern digital age.

Recommendations

Based on the findings demonstrated above, it is recommended that the Jordanian legislator amend the text of Article (7) of the Penal Code and Article (38) of the Cybercrime Law to include the principle of regional jurisdiction for

attempts to commit cybercrimes that occur abroad and do not result in a criminal outcome within the Jordanian territory due to reasons beyond the control of the cybercriminal. This should be done while excluding the residence requirement for cybercriminals to fall under the principle of universal jurisdiction. Instead, it should suffice to consider presence or transit, as stipulated in Article (10/4) of the Penal Code. We also urge the Jordanian legislator to amend Article (9) of the Jordanian Penal Code to expand the scope of crimes subject to the principle of personal jurisdiction to include all cybercrimes committed by Jordanians or foreigners abroad, whether they are felonies or misdemeanors.

Moreover, it is essential to add a provision to the Jordanian Cybercrime Law governing the situation of stateless or unknown nationality cybercriminals. This provision should stipulate the adoption of jurisdiction according to the law of the state to which they are connected in terms of residence and domicile. It is also recommended that the international legislator establishes a specialized court to handle cybercrimes, considering the uniqueness of these crimes and the absence of a specialized judicial body to address acts of electronic aggression carried out by states against each other, or at the very least, consider redefining the crime of aggression as stipulated in Article (8) of the Rome Statute of the International Criminal Court to include cyberattacks.

References

Abdel-Al, Muhammad Okasha, (2007), *Provisions of Lebanese Nationality*, Al-Halabi Legal Publications, Beirut, Lebanon.

Abdul Qadir, Waddah Ghassan, (2022), State Sovereignty and its Impact on Disrupting the Rule of Conflict of Laws, *Iklil Journal for Human Studies*, 9, 769-786.

Al-Badri, Abdullah Mazen Badr, (2022), *The Role of Will in Losing and Reclaiming Nationality,* Master's Thesis, Faculty of Law, Middle East University.

Al-Ghata, Ali Adel Kashif, and Al-Shammari, Marwa Youssef Hassan, (2012), The multiplicity of crimes and its impact on punishment, a comparison between Iraqi, Egyptian, and Jordanian legislation, *Journal of the University of Kufa*, 26, 209-227Iraq.

Al-Hadid, Nour Mazen Muhammad, (2014), *Dual citizenship in Jordanian legislation*, Master's thesis, Faculty of Law, Middle East University.

Al-Jubouri, Ibrahim Abbas, (2020), Applying the rules of conflict of laws - the rules of attribution - according to the position of the Iraqi legislator, *Journal of the College of Basic Education for Educational and Human Sciences*, 47, 1058- 1069 Iraq.

Al-Saadi, Karim Mazal, (2005), The concept of the rule of attribution and its characteristics - a comparative study in conflict of laws, *Journal of Karbala University*, 3(13), 1-28, Iraq.

Al-Shawabkeh, Muhammad, (2004), *Computer and Internet Crimes*, 1st edition, Dar Al-Thaqafah, Jordan.

Badie, Sami, and Al-Ajouz, Osama, (2013), *Private International Law*, 3rd edition, Zein Law Publications, Beirut, Lebanon.

Benslimane, Abdel Salam (2017), *Cybercrime in Moroccan Legislation: a critical comparative study in light of the opinions of jurisprudence and judicial rulings*, Dar Al-Aman, Rabat, Morocco.

Cybercrime Law No. (27) of 2015.

Egyptian Civil Law No. (131) of 1948.

French Civil Code.

Hijazi, Abdel Fattah Bayoumi, (2007), *Combating Computer Crimes in the Model Arab Law*, Dar Al-Kutub Al-Qanuni, Cairo, Egypt.

Iraqi Civil Law No. (40) of 1950.

Jaber, Abd al-Rasoul Abd al-Rida, (2007), The Role of the Region in Determining the Applicable Law, *Babel Journal of Human Sciences,* 14(2), 156-166, Iraq.

Jamil, Abdel Baqi, (2010), *The Internet and Criminal Law, Substantive Provisions for Internet-related Crimes*, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

Jordanian Civil Law No. (43) of 1973.

Jordanian Penal Code No. (16) of 1960.

Khalifa, Muhammad, (2016), The specificity of electronic crime and the efforts of the Algerian legislator to confront it, *Arab Journal of Research in the Humanities and Social Sciences*, 25(1), 270-289

Khansaa, Saadi, (2010). The implications of information and communications technology on the organization and its social environment. *The journal of law and human Sciences*. 23 (2), 85-103.

Mahmoud, Raad Miqdad, (2021), The applicable law in the event of a conflict of nationalities - a comparative study, *Tikrit University Journal of Law*, fifth year, 5(4), 45-69, Iraq.

Maidan - Today's latest news: Al Jazeera Net (2023) Al Jazeera Net: *Today's latest news around the world.* Available at: https://www.aljazeera.net/midan/miscellaneous/technology (Accessed: 20 July 2023).

Nassif, Safaa, (2016), Procedural Challenges Related to Information Crimes, *Journal of Legal and Political Sciences*, 5(2), Ain Shams University, Cairo, Egypt.

Shayen, Nawal, (2022). Cybercrime in Algerian legislation - its nature, subject, and characteristics. *University Batana*, Algeria. 2 (6), 59-80.