Pakistan Journal of Criminology
Vol. 15, No. 04, October-December 2023 (69-85)

The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes?

Tawfiq Khashashneh[1], Tareq Al-Billeh[2],
Ali Al-Hammouri[3] & Roua Belghit[4]

Abstract

In the current investigative process, digital technology has become an essential tool that helps forensic specialists and law enforcement organizations retrieve electronic evidence that is vital to solving crimes. Obtaining electronic evidence from crime scenes is seen as a challenging investigative task, particularly in light of the rise in cybercrime techniques. In order to find some hints or evidence or assess their significance using scientific and technical data that neither the judge nor the investigator have access to, it takes professional investigators and technical experts. This study examines the value of digital technology in the recovery of electronic evidence and its practical use at crime scenes. Through an analysis of many methodologies, instruments, and obstacles, this research illuminates the dynamic field of digital forensics and its function within the criminal justice structure.

Keywords: Crime Scene, Digital Technology, Evidence, Electronic Evidence, Cyber Crime

Introduction

In the current era of growing digitalization, electronic evidence has emerged as a crucial element in criminal investigations. The previous several decades have seen incredible scientific advancements in the realm of information technology, leading to an electronic revolution that is now pervasive in all facets of daily life. It has become extremely difficult to do without its unlimited services. However, there are some mentally ill people who have exploited these advanced methods to commit many crimes, using the enormous potential of these innovations. The rates of these crimes have increased during the last two decades, in a way that has led to the emergence of new criminal phenomena known as information crime

[1] The Author is an Assistant Professor at the Faculty of Law at the Ajloun National University, Ajloun, Jordan. He can be accessed on t.khashasheh@anu.edu.jo t_khashashneh@yahoo.com
[2] The Author is an Assistant Professor at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, and the author is a practicing lawyer in Jordan as well. He can be accessed on t_billeh@asu.edu.jo
[3] The Author is an Assistant Professor at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, and the author is a practicing lawyer in Jordan as well. He can be accessed on a_alhammouri@asu.edu.jo
[4] The Author is an Assistant Professor at the Faculty of Law at Larbi Tebesi University, Tebessa, Algeria. He can be accessed on Belghit.roua@univ-tebessa.dz

or electronic crime (Al-Thunaibat, 2003). Organized crime was carried out using the Internet, including electronic fraud by tampering with inputs and programs, illegal copying of programs, and many crimes related to electronic commerce. Crimes are also committed by destroying electronic devices and computer records, broadcasting pornographic images and films, defamation and insults via e-mail, and money laundering using electronic money (Hosni, 1998).

The danger of these new criminal phenomena is that the crime is easy to commit by or through these devices. Its implementation does not take a long time, but in many cases, it is completed in a few seconds. Likewise, erasing traces of the crime and destroying its evidence is often resorted to by the perpetrator after committing the crime (Aqida, 2004). Considering this development in the methods of committing crimes, discovering the perpetrator has become difficult. Therefore, it has become necessary for the same weapon to be used using modern digital technology to detect crime and collect evidence from the cybercrime scene (Al-Zaabi, 2014).

Scientific evidence has become an effective means of finding the link between the crime and the perpetrator and reducing the chances of error in criminal proof and judicial rulings. Hence, scholars of jurisprudence and law rushed to create new rules to govern modern technology by updating and amending laws, especially the laws of criminal procedure and the laws of criminal evidence (Bin Younis, 2004). This development paved the way for a new dawn of scientific evidence. Reliance on the forensic laboratory, scientific equipment, and advanced digital technology has increased day after day. Evidence derived from imaging devices, speed measuring devices, genetic fingerprinting, computers, and various other scientific methods has become acceptable and approved today before the courts.

It is hardly hidden from anyone the importance of researching all aspects related to dealing with electronic evidence, given the widespread of these crimes. Crime has begun to spread, with its effects overriding those of traditional crimes. Hence, criminal jurisprudence took it upon itself to research some of the details related to cybercrimes, including the procedures related to inspecting the cybercrime scene and collecting evidence from it.

The role of digital technology in cybercrime scenes is of great importance. It was an incentive to choose it and take it up with research and study. This importance is demonstrated by its close and direct connection to the phenomenon of cybercrime, which has begun to appear and spread recently. It is considered one of the thorny topics that have occupied the minds of criminal law jurists, given the transition of societies and countries to the information age and the increase in interconnectedness through electronic communication networks. This made it easier to commit crimes by means that were not common before. There appears to be an

urgent need to confront this wave of unconventional crimes. This is done with advanced scientific technology, and the development of modern legislation, whether punitive or procedural, that addresses these problems (Abdel Muttalib & Zubaida & Abdel Aziz, 2003).

Given the special nature of the electronic crime scene, the difficulties, and complex steps that the criminal investigator may face to conduct the electronic examination in order to obtain evidence, which, as we know, is stored in electronic means, it can be manipulated and change the truth that we seek. Therefore, the research problem can be summarized in the fact that the use of digital technology in electronic crime scenes constitutes a new challenge for the authorities to search and investigate crimes (Rostom, 1994).

Accordingly, it is necessary to answer the problem of the study and return it to its primary elements according to the following questions: How can digital technology be used at crime scenes? How can evidence be extracted from a cybercrime scene? The use of digital technology for evidence extraction has gained immense importance in solving crimes. This paper aims to highlight the pivotal role of digital technology in extracting electronic evidence and offers insight into how it can be effectively employed at crime scenes.

Methodology

In this research, we were keen to adopt a logical approach. Therefore, the research relied on the descriptive-analytical method. This approach aims to describe and diagnose various topics in all their aspects and dimensions, not limited to the theoretical aspect only. Rather, the applied aspect will be present in this research. Traditional rules of criminal and procedural law will apply to cybercrimes. This will be done by analysing the facts and information related to those topics under research and study, as their vocabulary and components were analysed and reduced to their primary elements to extract the most important rules and provisions related to the topic.

Role of technical expertise in extracting electronic evidence

There is no doubt that extracting electronic evidence from crime scenes is considered a complex investigative work, especially considering the increase in digital electronic criminal methods. It requires specialized investigators and technical experts who can be used by the judge to uncover some clues or evidence or determine their significance using scientific and technical information that is not available to the investigator or judge (Othman, 1964; Adel Ghanem, 1968; Hosni, 1998; Al-Thunaibat, 2003).

a. Importance of technical expertise at the cybercrime scene

In the context of modern crimes that take on a digital, electronic nature, in such crimes, technical expertise is an essential element to determine how the crime was committed from a technical angle. It is also to identify what could be a new technology that will benefit the judiciary and the possibility of its acceptance in the law. This is the direction taken by the Paris Court in the case Union of Jewish Students and Lycra v. Yahoo. It sought the help of Internet experts to learn about the possibility of determining a security path using filtering (Al-Zaabi, 2014; Bin Younis, 2004; Al-Billeh, 2022a). The importance of experience in cybercrime scenes is clear because computers and communication networks come in many types and models. Likewise, the sciences and technologies related to them belong to precise and diverse scientific and technical specializations. Some define technical expertise (Othman, 1964; Al-Billeh, 2022b): as the technical advice that a judge or investigator seeks to help him from his belief regarding issues whose assessment requires knowledge, or special scientific knowledge that he does not have.

For our part, we see the importance of the criminal investigator or judicial police officer being familiar with the types of cybercrimes as well as the experts and specialists in this field. This is for the purpose of selecting and assigning the expert whom he deems competent to be guided by his technical expertise and skill. The judge cannot decide on purely technical issues without consulting the opinion of experts (Hosni, 1998; Al-Billeh, 2022c). If the judge addresses the technical issue and decides on it without a technical expert, his ruling is flawed and must be overturned. This principle was settled by the judges of the Egyptian Court of Cassation (Aqida, 2004; Al-Billeh, 2022d).

b. Technical rules governing the work of the electronic (technical) expert

Technical means are of utmost importance in deriving electronic evidence from a crime scene. They are no less important than the legal rules. However, these rules are specific and unique to technical expertise. The most important methods used in the field of electronic expertise are the following (Rostom, 1994; Al-Billeh, 2022e):

- Description of the computer's installation, make model, type of operating system, and the most important subsystems it uses, in addition to the devices attached to it, the password, and the encryption system.
- Description of the computer or network environment in terms of organization, extent of concentration or distribution of automated processing work, type of means of communication, frequency of broadcast waves, and locations of their storage.

One of the practical applications that illustrates the importance of the role of the technical expert in the field of network crimes is a case whose facts are summarized as follows (Al-Husseini, 2012; Corrias, 2023).

As for the steps to derive evidence from the cybercrime scene, it is considered one of the most difficult matters facing the cyber expert. The most important steps to derive this new evidence are the following stages (Abdel Muttalib & Zubaida & Abdel Aziz, 2003):

First: Pre-operation and inspection steps

- Ensuring that the contents of the seized items are identical to what is written on them.
- Ensuring that the system units are fit for operation.
- Recording the data of the seized units and components, such as type, model, and serial number.

Second: Operation and inspection steps

- Using the recording of the rest of the data through the device readings.
- Making a copy of all the seized storage media, especially the hard disk, to conduct an initial examination on this copy to protect the original from loss, damage or destruction, whether due to misuse or the presence of viruses or programming bombs.
- Identifying the types and names of software groups, system programs (operating programs), application programs, communications programs, and other programs related to the subject of the crime, such as programs for creating and processing images in child prostitution crimes, for example.
- Showing hidden files and texts inside images.
- Recovering files that were originally deleted using data recovery programs, as well as broken or damaged files such as Recover Man Professional Easy Recover.

These files or data are then stored, another exact copy of the CD or disk containing them is made for examination by applying the above-mentioned steps.

A list is prepared in which the technical expert takes an inventory of all the electronic evidence obtained on his disk, while reviewing each image kept on the disk in another computer to ensure the integrity of the list.

The electronic evidence is converted into a physical form by printing the files, photocopying their content if they are images or texts, or placing them in any other container depending on the type of data and information that make up the evidence.

c. How the electronic expert works

The technical expert in the field of searching for evidence at the cybercrime scene must do everything he can to reach the truth and uncover it. He has the right to use the scientific methods he acquired and learned in his specialty to perform his work tasks. The court may not reject these methods unless the rejection is justified and logical, otherwise, the ruling will be subject to cassation. There are two methods for the electronic expert's work (Bin Younis, 2006):

First method: inventorying and compiling sites that constitute a crime in and of themselves, as is the case with sites of threats, fraud, insults, and defamation, or crimes of copying and broadcasting obscene images with the intention of propaganda to incite the commission of crimes of prostitution, slavery, child prostitution, and others. Then it conducts an electronic digital analysis of these sites to find out how they were prepared programmatically, and to attribute them to the path from which they were issued or prepared. The elements of its movement are also identified, and how was its knowledge achieved? Then, in the end, the IP that is attributed to the computer that issued these websites is achieved. Browsing tracking, in particular, allows anyone who looks at it to know the computer's IP address. The local route to the network supplying the browsing traffic is thus traced. Then the physical address of the subscriber in the network is reached. Such a matter helps in identifying the person who deals with the computer and establishes the assumption that the person who dealt with it is its owner, especially if the individual here is a natural person (Bin Younis, 2006).

Second method: inventory and compilation of a group of sites whose subject matter does not constitute a crime. Rather, it leads those who are curious, if they follow its subject, to commit crimes and slip into crime, directly or indirectly. This is also the case with websites that help others identify the doses of drugs and psychotropic substances that are appropriate for a person's weight, if if the instructions contained therein are followed, they will not lead the person to a state of addiction, and so on. In addition to sites that explain how to grow drugs away from the eyes of others. Also, how to prepare and store bombs, and how to deal with time bombs, install them, dismantle them, and store them.

Likewise, specifying the route of entry to a prostitution site from different places without the necessity of entering from fixed places. As if the perpetrator of the crime subscribed to a provider in a city other than the one in which he resides (Al-Thunaibat, 2003). In this context, these sites can be tracked, and electronic evidence can be obtained.

The third method: is preserving electronic evidence of transport, network, and communications protocols from routine operations that require accuracy. It sometimes poses a relative difficulty from the point of view of evidentiary and investigative bodies, and thus law enforcement agencies (Al-Feki, 2013). The difficulty is when this evidence and these files are mixed with other files of information of innocent computer users, which may pose a threat to their privacy. Therefore, they may often end up being released, not seized, and returned to their owners if it is not relevant to the crime committed (Al-Ghaferi, 2007; Fox & Yamagata, 2022).

As for the process of preserving evidence in the electronic world, it requires the technical expert to monitor and inspect the Internet site, or information that indicates the crime, which takes various forms. As if the crime were one of insults and slander in discussion rooms. In this case, the memory of the server who is responsible for connecting these rooms through the digital world is resorted to, so that it is possible to determine the subject of the insult and slander and its history. However, if the crime is one of online publishing, it may suffice to resort to inspecting the memory of the computer used only without the need to specify the server. In such cases, the technical expert uses auxiliary software to achieve preservation in the digital world. This is also the case with blocking and encrypting such sites after determining their path. This would result in him not being able to delete it from the digital world; otherwise, it would be considered evidence that he committed the crime (Al-Zaabi, 2014).

The expert also has the right to learn about the style of the cybercrime perpetrator by interviewing him based on his statements, and to review the testimonies and statements of the perpetrators before official authorities and others. This is to have an idea of how to deal with electronic evidence, which they may leave behind in the virtual world and so on (Al-Ghayathin, 2013; Freitas, 2017). In this regard, the US Congress summoned one of the most prominent hackers in the virtual world, even the most dangerous of them all, "Kevin Fink," to testify as a hacker about how he committed the hack and his opinion on preparing legislation prohibiting hacking. His testimony included many matters that were hidden from the jurists. Rather, it is a certificate that is considered a legislative precedent in this field (Al-Thunaibat, 2003; Alkhseilat et al., 2022).

Extracting and storing electronic evidence from the crime scene

The judicial police employee assigned to inspect the cybercrime scene must write a report listing the seized electronic evidence and its distinct descriptions. This

evidence is placed in a locked safe, especially since the forms of this evidence are many and varied, including documents, photographs, e-mails, video clips, contact lists, electronic spreadsheets, databases, instant messages, chat logs, etc.

a. Legal rules for preserving electronic evidence.

Both the Jordanian legislator and the Egyptian legislator were keen to clarify the instructions for dealing with and documenting evidence. Article 87 of the Jordanian Code of Criminal Procedure stipulates: "The public prosecutor shall be accompanied by his clerk and seize or order the seizure of all things he deems necessary to reveal the truth. He shall compile a record of them and keep them in accordance with the first paragraph of Article (35). Article (56) of the Egyptian Code of Criminal Procedure also stipulates that items should be tied whenever possible, sealed, and the date of the report drawn up to seize the items written on a strip inside the seal. The subject for which the seizure occurred is also indicated.

The intention of these procedures is to protect the seized items from damage, tampering with or alteration. In this regard, Article (88) of the Code of Procedure stipulates that: "The public prosecutor may seize at post offices all letters, newspapers, publications, and parcels, and all telegraphic messages at telegraph offices. He may also monitor telephone conversations whenever this is useful in revealing the truth."

Correspondence here means all written letters, whether sent by mail or by a private messenger. It is the same for the message to be inside a closed or open envelope or to be on an open card, as long as it is clear from the sender's intention that he did not intend for others to see it without discrimination (Al-Thunaibat, 2003; AL-KHAWAJAH et al., 2022). It is worth noting that the legal rules that regulate the process of preserving electronic evidence are intended to regulate the work to preserve the evidence for fear of it being lost. Thus, the evidence is safe from tampering with before presenting it to the court.

Therefore, it is important for the team charged with collecting electronic evidence from the crime scene to make an effort to preserve and store it in a safe environment that does not lead to its damage. The Spanish scientist Victor Cardenes discovered a type of fungus that feeds on well-known compact discs (CDs), which are considered the most popular method for circulating computer programs, songs, music, and various types of technical means (Al-Thunaibat, 2003; ALMANASRA et al., 2022).

This fungus destroys all the data loaded on these discs, leading to their loss forever. It also makes them worthless and useless cylinders. Therefore, no CD-reading device can read its contents, even though they are preserved in the usual

and recognized way (Hosni, 1998; Alshible et al., 2023; Al-Billeh et al., 2023; Longo & Lorubbio, 2023).

Therefore, it is important to know that what is meant by seizing evidence is: placing the items and papers that are seized in a closed safe, tied whenever possible, and sealed. The date of the report drawn up of the seizure of those items is written on a strip inside the seal. The subject for which the seizure took place is also indicated. Evidence seized in crimes in general and crimes committed via computer networks, in particular, are considered important in determining conviction or acquittal. Therefore, attention must be paid to the process of storing the seized electronic evidence in the electronic environment (Al-Thunaibat, 2003; Isa et al., 2022; Al-Billeh & Al-Qheiwi, 2023).

b. Tools for filing electronic evidence.

When the competent expert documents the electronic evidence, a distinction must be made between the evidence. 2.2 Tools for filing electronic evidence. When the competent expert documents the electronic evidence, a distinction must be made between the evidence. There is some evidence that is subject to loss and some that is not. It is also possible to distinguish between evidence that must be preserved inside the computer and that which must be preserved outside the computer, as well as the evidence that must remain in the virtual world. There is also evidence that belongs to the digital world that can be taken from the digital framework inside computers to the physical world. They are treated as outputs that become acceptable before the judiciary as complete evidence of the crime. Here it is necessary to recognize the types of this evidence as follows:

First: Evidence or data that is vulnerable to loss:

It is within RAM and includes:

- Details about network settings.
- Open or closed network connections.
- Open files and running applications.
- Current users.
- Chat logs.
- Email messages.
- Passwords and encryption keys.

Second: Evidence and data that are not at risk of loss (Abu Issa, 2014):

- Internal hard disks.
- External hard disks.
- Hard disk and CD/DVD.
- Memory cards.
- USB thumb drive

-Digital Camera.
- MP3 players.
- Cell phones.

As for how to preserve and collect evidence and data that are not at risk of being lost, they are as follows (Abu Issa, 2014):

- Address cards
- Ink pens and markers.
- Storage containers.
- Anti-static bags.
- Rubber gloves.
- An additional camera and film (video camera if available).
- Notebook.
- Blank discs.
- Evidence tape.

It should be noted that the evidence, whether it is at risk of being lost or otherwise, is wise to keep it outside the computer. Others we can preserve inside the computer, or preserve in the digital world using some programs designed for this purpose, as follows:

- **Preserving the electronic evidence outside the computer (Al-Thunaibat, 2003; Al-Billeh & Abu Issa, 2022)**: This is done by using special equipment to protect the various storage media (hard disks, flash memory, various memory cards,). Thus, digital evidence is preserved from being changed, modified, or deleted. It allows digital evidence to be read and written on.
- **Preservation inside the computer (Hosni, 1998):** The process of preserving electronic evidence inside the computer is carried out in several ways, the simplest of which is represented by using the normal preservation method. Its strongest manifestations are in computer seizure operations on the evidence placed in it. Digital evidence is usually a file containing digital data that gives a specific informational appearance that cannot be transferred to another appearance, except after making digital modifications to the aforementioned data.
- **Preservation in the digital world:** This requires the electronic technical expert to monitor information that indicates the crime. This is done by monitoring Internet sites or any sites that indicate the presence of information about the occurrence of a crime. For example, the crime was one of insults and defamation in the discussion room. In such a case, the memory of the server which is responsible for connecting these rooms through the digital world is resorted to so that it is possible to determine the

subject of the insult and defamation and its history. Or the expert uses some software to achieve the feature in order to assist in preservation in the digital world. As is the case in online publishing crimes, it may be sufficient to simply resort to the memory of the computer being used without the need to specify the server (Hosni, 1998; Khashashneh et al., 2022; AL-Hammouri et al., 2023; Al-Billeh, 2023).

It should be noted that many investigative authorities and courts are in the process of preserving this evidence digitally. It is delivered to a specialized department, which in turn preserves the evidence in the digital world to present it to the judiciary whenever necessary. This requires the technical expert to present this evidence to the court at a certain stage. It also makes the expert's work often representative of the post-trial stage (Al-Thunaibat, 2003; Al-Hammouri & Al-Billeh, 2023).

c. Extracting electronic evidence.

This requires the technical expert to extract digital evidence from various electronic devices, storage media, and computers of all types. It also includes cellular devices when there is suspicion of a criminal act in which electronic means such as computers were used in the implementation process. Or information was stored or hidden that would be useful in investigations, inferences, and proof of the criminal act, especially in cases of falsification, counterfeiting, cell phone cases, and others.

It should be noted that the technical expert can use the following devices and equipment in the process of extracting electronic evidence (Abu Issa, 2014; Al-Billeh et al., 2023):

- Fixed and portable forensic stations for examining and analysing electronic evidence with the systems (FTK, Encase), as is practiced in the most developed countries of the world.
- Special equipment to protect various storage media (hard disks, flash memory, various memory cards, etc.) and preserve the digital evidence from change, modification, or deletion, as it allows the digital evidence to be read or prevents writing on this evidence.
- Equipment for physically copying hard disks.
- The Rainbow system for decrypting and protecting passwords, including complex ones.

d. Securing electronic evidence extracted from the crime scene.

Seized digital electronic evidence is crucial to determining guilt or acquittal. So, the team examining and collecting evidence from the cybercrime scene must try

to preserve it and store it in an appropriate environment that does not spoil it. Therefore, it becomes vulnerable to damage and is inadmissible as evidence before the competent judicial authorities.

Before carrying out the process of storing evidence at the electronic crime scene, the inspection team must remember the following (Abu Issa, 2014; Al-Billeh & Al-Hammouri, 2023):

- If your computer is off, leave it that way.
- Do not attempt to access data if you are not qualified or an expert.
- Identify potential sources of electronic evidence or storage media.
- Keep everyone away from the intended or targeted crime scene's computer, cell phone or storage media.
- Know whether the intended computer can be accessed or not.
- Determine whether or not there is off-site data storage.
- Identify the suspect, victim, witness, system, hardware, software, email, and chat rooms.
- Document the crime scene: creating a permanent record of the scene and recording both digital and traditional evidence.

Examples of electronic evidence storage methods and related locations include the following (Sorour, 2014; Al-Billeh & Abu Issa, 2023; AL-KHALAILEH et al., 2023; Al-Khawajah et al., 2023; Reiling & Contini, 2022):

- **Preserving compact discs (CD):** Place the CD inside a plastic bag or inside a plastic box or cardboard cover. It is preferable to use nylon reinforced with air bubbles (Abu Issa, 2014). Seek the help of a computer expert to ensure the integrity of the CD and that there are no scratches on the surface of the cylinder.

Conclusion

The importance of digital technology in extracting electronic evidence cannot be overstated in contemporary criminal investigations. Its use at crime scenes and throughout the investigative process has revolutionized the field of forensics. The cybercrime scene is characterized by its cross-border and cross-national nature. There are no borders that stand in the way of the transfer and movement of information across different countries. Modern technology, computers, and their networks penetrate time and space without being subject to border guards. The world has indeed changed, and geographical borders no longer represent an obstacle to the movement and transmission of information.

Therefore, attention must be given to training experts, investigators, and judges to deal with cybercrimes of a complex technical and scientific nature. This training enables them to understand and investigate the cases presented to them, use

scientific methods at cybercrime scenes, deal with electronic evidence, and bring the truth closer to the judicial truth. Also, to formulate procedural texts for organizing and using modern technologies in detecting cybercrimes, using them at cybercrime scenes, extracting digital evidence, and dealing with it to be acceptable evidence before the judiciary. The successful integration of digital technology in crime scene investigations not only aids in solving crimes but also ensures the fair and just administration of justice.

References

Abdel Muttalib, M., Zubaida, J., & Abdel Aziz, A. (2003). *An proposed model for the rules for adopting digital evidence to prove crimes via computer*. Egypt: Electronic Banking between Sharia and Law Conference.

Abu Issa, H. (2014). *Principles of Criminal Trials, Volume One, The Theory of Criminal Evidence*. Amman: Dar Wael for Publishing and Distribution.

Adel Ghanem, A. (1968). Experience in the Field of Criminal Evidence. *Public Security Journal Research*, 43(1), 1-19.

Al-Billeh, T. (2022a). Judicial oversight on the administrative contracts in the Jordanian legislation and the comparison: the modern qualitative jurisdiction of the administrative judiciary. *Indian Journal of Law and Justice*, 13 (2), 1-28. https://ir.nbu.ac.in/handle/123456789/4763

Al-Billeh, T. (2022b). The Correction of the Invalidity of the Civil Trials Procedures in Jordanian and Egyptian Legislation: The Modern Judicial Trends. *Kutafin Law Review*, 9 (3), 486-510. https://doi.org/10.17803/2713-0525.2022.3.21.486-510

Al-Billeh, T. (2022c). Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. *Pakistan Journal of Criminology*, 14 (1), 1-14. http://www.pjcriminology.com/wp-content/uploads/2022/08/1.-Legal-Controls-of-the-Crime-of-Publishing-a-Program-on-the-Internet-in-Jordanian-Legislation.pdf

Al-Billeh, T. (2022d). Freedom of Religious Belief and the Practice of Religious Rites According to the Jordanian Legislation: Difficult Balance Between International and Regional Requirements as well as the National Legislative Controls. *Balkan Social Science Review*, 20. 117-137. https://js.ugd.edu.mk/index.php/BSSR/article/view/5503/4660

Al-Billeh, T. (2022e). The Impact of the Comprehensive Ban Due to the COVID-19 Pandemic on the Quality of Ambient Air in Jordan. Study for 15th March to 15th April of 2020 Period. Journal of Environmental Management and Tourism, 3(59), 802-811. https://doi.org/10.14505/jemt.v13.3(59).19

Al-Billeh, T. (2023). Disciplinary Measures Consequent on the Judges' Misuse of Social Media in Jordanian and French Legislation: A Difficult Balance between Freedom of Expression and Restrictions on Judicial Ethics. *Kutafin Law Review*, 10(3), 681–719. https://kulawr.msal.ru/jour/article/view/224

Al-Billeh, T., & Abu Issa, H. (2022). The Community Penalties in the Jordanian Criminal Law: What are the Alternatives to Liberty-Depriving Penalties? *Pakistan Journal of Criminology*, 14 (3), 1-18. http://www.pjcriminology.com/wp-content/uploads/2023/03/1.pdf

Al-Billeh, T., & Abu Issa, H. (2023). The Role of the Environment Committees in the Nineteenth Parliament for the Year 2020 in Studying Matters Related to Environmental Affairs in Jordan. *Journal of Environmental Management and Tourism*, 1(65), 168-175. https://doi.org/10.14505/jemt.14.1(65).16

Al-Billeh, T., & Al-Hammouri, A. (2023). Guarantees of Juvenile Trial Procedures in Jordanian Legislation: The International Standards towards Reformative Justice for Juveniles. *Pakistan Journal of Criminology*, 15 (1), 1-16. https://www.pjcriminology.com/wp-content/uploads/2023/07/1.Tareq_Billa_Paper_Final_Draft.pdf

Al-Billeh, T., & Al-Qheiwi, M. (2023). OBJECTION OF THIRD PARTIES OUTSIDE THE LITIGATION IN ADMINISTRATIVE JUDICIAL JUDGMENTS IN THE JORDANIAN AND FRENCH LEGISLATION. *Revista Relações Internacionais do Mundo Atual*, 4(42), 76-101. http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/e-5951

Al-Billeh, T., Al-Hammouri, A., Al-Khalaileh, L., & Derbal, I. (2023). The Impact of Administrative Control Authorities on Sustainable Development in Jordanian Legislation: What are the Challenges Facing Administrative Control Authorities in Achieving Sustainable Development?. *Journal of Law and Sustainable Development*, 11(5), e1129. https://doi.org/10.55908/sdgs.v11i5.1129

Al-Billeh, T., Alkhseilat, A., & AL-Khalaileh, L. (2023) Scope of Penalties of Offences in Jordanian Public Office. *Pakistan Journal of Criminology*, 15 (2), pp. 341-356, https://www.pjcriminology.com/publications/scope-of-penalties-of-offences-in-jordanian-public-office/

Al-Feki, A. (2013). *Criminal Proof of Crimes Committed via the Internet*. PhD Thesis. Ain Shams University.

Al-Ghaferi, H. (2007). *Criminal Policy Confronting Internet Crimes*. PhD Thesis. Cairo University.

Al-Ghayathin, M. (2013). Transnational Information Crimes. PhD Thesis. Cairo University.

Al-Hammouri, A. & Al-Billeh, T. (2023) Specificity of Criminalisation in the Jordanian Environmental Protection Law. *Pakistan Journal of Criminology*, 15 (2), pp. 357-371, https://www.pjcriminology.com/publications/specificity-of-criminalisation-in-the-jordanian-environmental-protection-law/

AL-Hammouri, A., Al-Billeh, T., & Alkhseilat, A. (2023). The Extent of Constitutionalizing the Environmental Rights as One of the Anchors to Keep a Healthy, Clean Environment: A Difficult Balance between the International Agreements and the Jordanian Constitution's Restrictions. *Journal of Environmental Management and Tourism*, 1(65), 89 -97. https://doi.org/10.14505/jemt.v14.1(65).09

Al-Husseini, A. (2012). *Procedural Aspects of Crimes Arising from the Use of Electronic Networks*. PhD Thesis. Ain Shams University.

AL-KHALAILEH, L., MANASRA, M., Al-Billeh, T., ALKHSEILAT, A., ALZYOUD, N., & AL-KHAWAJAH, N. (2023). Legal Regulation of Civil Liability for Environmental Damage: How Appropriate are Civil Liability Provisions with the Privacy of Environmental Damage?. *Journal of Environmental Management and Tourism*, 14(5), 2174 - 2186, https://doi.org/10.14505/jemt.v14.5(69).02.

Al-Khawajah, N., Al-Billeh, T., & Manasra, M. (2023). Digital Forensic Challenges in Jordanian Cybercrime Law. *Pakistan Journal of Criminology*, 15 (3), 29-44. https://www.pjcriminology.com/publications/digital-forensic-challenges-in-jordanian-cybercrime-law/

AL-KHAWAJAH, N., ALKHSEILAT, A., AL-BILLEH, T., MANASRA, M., & ALWERIKAT, N. (2022). Criminalization of the Transmission of the Coronavirus COVID-19 and Its Impact on the Right to a Healthy Environment. *Journal of Environmental Management and Tourism*, 13(7), 1881-1887. https://doi.org/10.14505/jemt.v13.7(63).08

Alkhseilat, A., Al-Billeh, T., Almanasra, M., & Alwerikat, N. (2022). Criminal Behavior as a Basis for Criminal Responsibility for the Crime of Introducing Substances Hazardous to the Environment in Jordanian Legislation. *Journal of Environmental Management and Tourism*, 7(63), 1851 - 1858. https://doi.org/10.14505/jemt.v13.7(63).05

ALMANASRA, M., Alkhseilat, A., Al-Billeh, T., ALWERIKAT, N., & ALSHARQAWI, A. (2022). Criminal Responsibility for the Crime of Discharging Polluting Substances for Water Sources in Jordanian Legislation. *Journal of Environmental Management and Tourism*, *13*(7), 1948–1948. https://doi.org/10.14505/jemt.v13.7(63).15

Alshible, M., & Abu Issa, H., & Al-Billeh, T. (2023). The Extent of Considering Environmental Crimes as A Manifestation of Economic Crimes. *Journal of Environmental Management and Tourism*, 1(65), 23-31. DOI:10.14505/jemt.v14.1(65).03

Al-Thunaibat, G. (2003). *The role of technical expertise in proving forgery in written documents in Jordanian law, comparative study*, PhD Thesis. Amman Arab University.

Al-Zaabi, M. (2014). *Crimes against reputation through electronic information technology, a comparative study*. Cairo: Dar Al-Nahda Al-Arabiya.

Aqida, M. (2004). *Investigation and Collection of Evidence in the Field of Cybercrimes*. Dubai: Research presented to the First Conference on the Legal and Security Aspects of Electronic Operations.

Bin Younis, O. (2004). *Crimes arising from the use of the Internet*. Cairo: Dar Al-Nahda Al-Arabiya.

Bin Younis, O. (2006). *Criminal Proof via the Internet.* Egypt: Research working paper, Digital Evidence Symposium at the headquarters of the League of Arab States in Egypt.

Corrias, L.D.A. (2023). Environmental Law and Youth Protests: Future Generations Between Speech Acts and Political Representation. *Int J Semiot Law*, 36, 893–906. https://doi.org/10.1007/s11196-022-09907-4

Fox, D., & Yamagata, H. (2022). Developing Court Capabilities and Insights through Data Conversion. *International Journal for Court Administration*, 13(1), 1-13. https://iacajournal.org/articles/10.36745/ijca.437

Freitas, M. (2017). Access to Environmental Justice in Brazil. *International Journal for Court Administration*, 8(3), 1-6. https://iacajournal.org/articles/10.18352/ijca.232

Hosni, M. (1998). *Explanation The Code of Criminal Procedure*. Cairo: Cairo University Press.

Isa, H. A., Alwerikat, N., & Al-Billeh, T. (2022). The Concept of the Public Employee in Jordanian Law: Different Constitutional, Administrative, and Criminal Law Definitions. *BiLD Law Journal*, *7*(2s), 331–337. https://bildbd.com/index.php/blj/article/view/318

Khashashneh, T., Al-Billeh, T., & Issa, H. A. (2022). THE AUTHORITY OF THE CRIMINAL JUDGE TO ASSESS DIGITAL (ELECTRONIC) EVIDENCE IN JORDANIAN, EGYPTIAN, AND FRENCH LEGISLATION. *Journal of Southwest Jiaotong University*, *57*(5), 631–640. https://doi.org/10.35741/issn.0258-2724.57.5.51

Longo, M., & Lorubbio, V. (2023). Ecosystem Vulnerability. New Semantics for International Law. *Int J Semiot Law*, 36, 1611–1628. https://doi.org/10.1007/s11196-023-09998-7

Othman, A. (1964). *Experience in Criminal Matters*. PhD Thesis. Cairo University.

Reiling, D., & Contini, F. (2022). E-Justice Platforms: Challenges for Judicial Governance. *International Journal for Court Administration*, 13(1), 1-18. https://iacajournal.org/articles/10.36745/ijca.445

Rostom, H. (1994). *Procedural Aspects of Information Crimes, A Comparative Study*. Assiut: Library of Modern Machines.

Sorour, A. (2014). *The Mediator in the Code of Criminal Procedure*. Cairo: Dar Al-Nahda Al-Arabiya.