Indonesian Journal of Law and Justice Volume: 3, Number 4, 2026, *Page*: 1-11

Identity Theft Crimes in E-Learning: A Comparative Legal Study in Light of Iraqi and Egyptian Legislations and International Conventions

Turath Mohammed Abdul Aziz

Northern Technical University

DOI:
https://doi.org/10.47134/ijlj.v3i4.6052
*Correspondence: Turath Mohammed Abdul Aziz
Email: turathalanaz@ntu.edu.iq

Received: 22-04-2026
Accepted: 22-05-2026
Published: 22-06-2026

Abstract: The rapid development of technology and the widespread use of e-learning has undoubtedly created new cybercrime varieties, including electronic identity theft crimes that directly threaten the security of digital educational institutions and the rights of students and faculty members. These crimes include the use by the perpetrator of the data, accounts, or electronic identity of another person to gain access to an educational platform without authorization, to commit fraudulent actions, or to access academic privileges without authorization. The gravity of these crimes is because they are easily committed using modern technology and hard to catch. The aim of this research is to identify the nature of the crime of identity theft in e-learning, to study the legal elements of that crime, the forms thereof and the consequences of the crime, as well as studying the position of Iraqi and Egyptian legislation and the relevant international conventions concerning the crime of identity theft. Finally, the study aims to present a general system of laws that will help to improve the level of protection of crime in the digital educational environment. The research follows a comparative analytical method, using the analysis of relevant legal documents, as well as comparing with legislation and international conventions, and also references legal jurisprudence and recent studies on the topic of the research.

Keywords: Identity Theft Crimes, E-Learning, Cybercrime, Criminal Protection, Digital Identity, Iraqi Legislation, Egyptian Legislation

Introduction

Electronic communication has become ubiquitous in recent years and technology has grown at an unprecedented rate in our lives. The education sector is one of the most impacted by this digital transformation, especially after the onset of the Covid-19 pandemic where schools had to implement an alternative educational system of e-learning and digital platforms. As a result, new variations of cybercrime have occurred in the electronic learning space, particularly, electronic identity theft crimes (Al-Kahwaji, 2002).

Identity theft crimes occur when someone uses another person's credentials or electronic accounts without proper permission to: gain unlawful access to educational systems; acquire academic privileges; or engage in fraudulent actions that jeopardize the integrity of the educational experience. Other than transnational nature which is the hallmark of a contemporary cybercrime, the ease of committing such crimes and the

challenges of their detection make them particularly dangerous (Mahmoud, 2002). Further, with the swift advancement of artificial intelligence technologies and deep fake techniques, the ways in which identities are being impersonated in the electronic educational context is becoming more complex. Now it is possible to fake voices, images and create fake digital personalities, making criminal proof and the evidentiary value of digital evidence more challenging. (Russel and Norvig, 2021)

This topic is becoming increasingly important, as electronic examinations and distance learning are becoming more common, and digital identity has become the main method of verifying the identity of a user in a learning environment. Therefore, any violation of it is a violation of the principles of digital trust and security of educational institutions. (Afify, 2000)

Research Significance

1. To explain what constitutes an identity theft crime in e-learning.
2. To elucidate the position of Iraqi and Egyptian laws about these offenses.
3. To evaluate the level of criminal protection of digital educational services.
4. To review and discuss the practical issues in relation to digital evidence.
5. To make legislative recommendations that help develop legal protection for digital identity.

Research Problem

The research problem can be formulated as the following question; "How effective is the Iraqi and Egyptian legislation, as well as international conventions, in combating identity theft crimes in e-learning and in giving sufficient criminal protection to digital educational platforms?"

There are several subsidiary questions this main question raises, such as:

- What is meant by the crimes of electronic identity theft?
- What are the elements and forms of these crimes?
- To what extent are traditional legal provisions adequate to address these crimes?
- What are the greatest practical issues with respect to digital evidence?

Research Objectives

1. To identify what electronic identity theft crimes are and their features.
2. To recognize the elements of these crimes.
3. To compare the location of Iraqi and Egyptian legislation in terms of crimes related to digital identity theft.
4. To Explore the Contribution of International Conventions to the fight against Cybercrime.
5. To suggest legislative and practical solutions that will enhance criminal protection in the electronic educational environment.

Methodology

The research method is comparative analytical, which involves analyzing the legislation in Iraqi and Egyptian laws regarding cybercrimes and then comparing it with the international conventions. It also is based on legal jurisprudence, current research and the examination of recent trends in relation to the protection of digital identity in e-learning.

Previous Studies

First: A Study by Abdulrahman Dakhel Nahi

The study examined the crime of electronic identity theft as one of the modern crimes resulting from technological development. It focused on the legal nature of the crime, its constituent elements, and methods of combating it under Iraqi legislation. However, it did not address the specific characteristics of the electronic educational environment as an independent subject of study.(Nahi, 2022)

Second: A Study by Suzan Kazem Khalaf

This study addressed the criminal protection of e-learning platforms and focused on crimes committed against educational platforms and the legal safeguards established for their protection. However, it did not provide a separate and comprehensive treatment of digital identity theft crimes within the e-learning environment(Khalaf, 2021).

Foreign Studies

Some recent foreign studies have focused on the protection of digital identity in electronic educational systems through the use of encryption technologies and blockchain applications. They have also examined the impact of artificial intelligence and deepfake technologies on the security of digital educational platforms(EduCTX).

Research Structure

The nature of the research necessitated its division into four sections: Section one deals with the nature of identity theft crimes in E-Learning. The second section addresses the legal response to electronic identity theft crimes. Section three, on the other hand, deals with practical challenges in proving electronic identity theft crimes. Finally, section four discusses the criminal liability arising from electronic identity theft crimes.

Result and Discussion

The Nature of Identity Theft Crimes in E-Learning

The Concept of Electronic Identity Theft Crimes

Electronic identity theft is the practice of one individual accessing another person's electronic data, information, or electronic accounts without authorization and using it for an unlawful purpose or to cause harm. There are several forms of this crime in the e-learning environment such as hacking university accounts, creating fake accounts in the name of the instructor or students, and illegally accessing the university's email accounts.(Hijazi, 2019)

In the electronic education environment, identity theft can also be characterized as "Any illegal act related to the use of someone else's electronic identity by a third party in

electronic learning environments with the intent to gain an academic advantage or to cause harm to the educational environment or its users." They have several characteristics, including technical in nature, easy to commit, hard to be traced by perpetrators and cross-border, making the prosecution of criminals more complicated. The researcher feels crimes of electronic identity theft are a double theft. They have the potential to infringe on digital privacy rights on one hand, and to compromise trust and security in the digital education landscape on the other. This requires special criminal protection that is suitable to their contemporary technological characteristics.

Elements of the Crime of Identity Theft in E-Learning

First: The Material Element

The actus reus of the crime of electronic identity theft is defined as any illegal act or activity involving the use or appropriation of another person's electronic identity without authority. This can be in the form of unauthorized access to educational platforms, hacking in to university email accounts, or creating fake accounts in electronic educational systems for illegal uses (Hijazi, 2005).

The criminal activity can be committed in many different ways, such as:

- Phishing.
- Hacking software and malicious programs.
- Password theft.
- Social engineering.
- Exploiting security vulnerabilities in educational platforms.

When the harmful action to the victim or educational institution is material, moral or academic, the criminal result is present. Some examples include altering an electronic examination, misusing data and information, or compromising the integrity of the educational institution's reputation and credibility. (Hijazi, 2005)

Second: The Mental Element

In order for the crime of electronic identity theft to be proven, the criminal element of knowledge and will must be both present. This means the perpetrator knows what he or she is doing is illegal and does it on purpose in order to gain some illegal advantage or to cause harm to the victim. (Al-Hadithi, 2010). Specific intent occurs when the person entitled to the grades, exam papers, academic data, and other academic advantages uses the digital identity of another person to acquire those advantages.

Forms of Identity Theft Crimes in E-Learning

Identity theft offenses in education are committed in a number of different ways and the most serious of these include:

1. Saving or copying student exams and then using the same identity to take an electronic exam.
2. Creating fake accounts in the names of faculty members.
3. Breaking into university email addresses.

4. Stealing students' academic information.
5. Manipulation of results of electronic exams (Baghdad Univ.).

In recent times, one such occurrence is the usage of generative AI and deep fake technologies to impersonate students or staff in online lectures or electronic exams. This presents legal issues concerning the authentication of eIDs and the admissibility of electronic evidence in court proceedings (Barfield and Pagallo, 2020). These crimes have grave implications that threaten the integrity of the educational process and the trustworthiness of academic credentials. They also ruin the reputation of educational institutions and lead to a loss of public trust in e-learning systems.

Legal Response to Identity Theft Crimes in E-Learning

Subsection One: Position of Iraqi Legislation

There is no comprehensive and fully implemented cybercrime law in Iraq. However, some laws can be used to combat electronic identity theft crimes, including the Iraqi Penal Code No. (111) of 1969 and the Electronic Signature and Electronic Transactions Law No. (78) of 2012. Article (456) of the Iraqi Penal Code (IPC) about the crime of fraud can be referred to in case the perpetrator deceived the educational institution through electronic means, or used digital data with the aim of taking an unlawful academic benefit. Similarly, provisions on forgery can be invoked if a fake account is created or an electronic document for an educational platform is forged. These provisions, however, were designed for traditional crimes and thus there is an issue about the adequacy of these provisions in dealing with the complex technical nature of the modern cybercrimes. (Al-Hadithi, 2010)

The researcher considers that the outdated rules provided in the Iraqi Penal Code are no longer adequate to meet the challenges of new ways of digital identity theft, especially in the context of e-learning, which is characterized by the wide variety of cyberattacks and the rapid development of technology. The draft Iraqi Cybercrime Law addresses issues concerning access to information systems, data theft, and unauthorized access. However, there is still need for the draft to be developed to conform with the latest technological advances. In fact, the Iraqi legislator has failed to adopt any laws to regulate digital identity theft crimes in the e-learning environment, due to the technical nature and complexity of the crimes and their speed, and cross-border aspects, which is different from the traditional nature of crimes as defined in the Penal Code.

As electronic identity theft continues to grow and evolve in the educational environment, there is growing need for special legislative measures to be taken in Iraq. Cybercrimes aren't just about stealing passwords these days or hacking into accounts; it's about using AI and deepfake technologies to create fake digital identities that are harder to identify using traditional methods. This makes the traditional penal measures inadequate to effectively tackle such contemporary crime trends. Beyond that, there is no clarity on the liability responsibilities of electronic educational service providers, creating questions of legal responsibility for the degree to which institutions are responsible for safeguarding academic information and users' digital identity. (Barfield and Pagallo, 2020)

Position of Egyptian Legislation

The Egyptian legislator has moved toward a clearer regulation of cybercrimes through the Information Technology Crimes Law No. (175) of 2018, which criminalizes unauthorized access to websites and electronic accounts, as well as the violation of the integrity of electronic data and information. The Egyptian law is characterized by its adoption of a modern concept of digital criminal protection, by criminalizing unauthorized access, attacks on private email accounts, and disruption of data and information. This allows its application to identity theft crimes within the e-learning environment even in the absence of a specific provision. Law No. (15) of 2004 on Electronic Signature also provides legal protection for electronic data and signatures and imposes penalties for unlawful appropriation or disruption of electronic media. (Egyptian Electronic Signature Law No. 15 of 2004.)

A comparison between Iraqi and Egyptian legislation shows that the Egyptian legislator has adopted a clearer digital criminal policy through the issuance of a specialized cybercrime law, whereas Iraqi legislation still relies on fragmented traditional provisions that do not fully accommodate the technical nature of these crimes. (Mansour, 2018)

It is to the credit of the Egyptian legislator that it has adopted a relatively proactive legislative policy in combating cybercrime by regulating digital evidence collection procedures and granting investigative authorities technical powers compatible with the nature of cyber offenses. Egyptian legislation, however, still needs to be more specific in protecting digital identity in educational institutions, especially with the current use of electronic examinations and educational distance learning technologies. This requires ongoing legislation to remain relevant with the latest technology. (Egyptian Anti Cyber and Information Technology Crimes Law No. 175 of 2018).

Position of International Agreements

The Budapest Convention on Cybercrime of 2001 is considered one of the most important international instruments addressing cybercrimes. It stresses the importance of making criminal acts involving the unauthorized access to information systems and altering digital information. Article 2 of the Convention makes it clear that it is a crime to illegally access information systems, and this will give an international basis for prosecuting electronic identity theft crimes through hacking accounts and educational platforms. The Convention has relevance in setting out rules for the cooperation of States with each other as well as with international organisations in combating transnational crimes, rules for the exchange of digital evidence and rules for mutual legal assistance between States, all of which contribute to minimising the transnational aspect of these crimes. A European Convention on Cybercrime was adopted in 2001. (European Convention on Cybercrime, 2001)

International accords on data protection and digital privacy also emphasize the need to provide effective protection of digital identity and to prevent its misuse in electronic environments, such as e-learning platforms. (UNTOC, 2000)

Practical Challenges in Proving Electronic Identity Theft Crimes

Subsection One: Difficulties of Digital Evidence

These crimes of electronic identity theft pose many problems in proving the crime, as they are highly technical and depend on high-tech electronic methods to hide the true identity of the person committing the crime. The most salient challenges are:

- Use of Virtual Private Networks (VPNs).
- Fake accounts.
- Risk of Digital Evidence being destroyed.
- Challenge in determining who's really responsible.
- The transnational nature of cybercrime.

The challenge of proof is even more difficult when a VPN is used or identity masking technology, as the perpetrator can be in a different geographic area or use a server outside the country where the crime was committed. Furthermore, cybercrime is a transnational phenomenon and this hinders international judicial cooperation, as well as the collection of digital evidence, especially when the servers or service providers are outside the jurisdiction of the investigating state. This can make it difficult to get access to evidence or to retain it because of the differing laws and policies in the various countries on data retention and digital records. The Budapest Convention on Cybercrime, 2001 (European Convention on Cybercrime)

Subsection Two: The Evidentiary Value of Digital Evidence

Digital evidence in identity theft crimes is comprised of:

- Email communications.
- Logs of e-learning platforms.
- Digital fingerprinting.
- Electronic recordings.
- Internet Protocol (IP) addresses.

A key question in criminal proof is the evidentiary value of digital evidence and its admissibility in court will rest, in part, on the technical integrity and protection of the digital evidence from alteration or tamper. The authenticity and reliability of it also does need specialized technical expertise. (Edwards, 2020)

Subsection Three: The Role of Technical Expertise and Digital Forensics

One of the key tools in establishing cybercrimes is technical expertise, with the courts increasingly turning to reports from cybersecurity experts and digital data analysts to review devices, electronic accounts, and track criminal activity. The researcher considers that the effectiveness of the criminal evidence in cases of identity theft must be formed the technical infrastructure of educational institutions and training of specialized personnel in the field of cyber-security and digital forensics.

Criminal Liability Arising from Electronic Identity Theft Crimes

Liability of the Principal Offender

The principal offender is liable for the costs of the recovery work. The principal offender must pay costs for the recovery work done. The principal offender is liable for the criminal offense if the person commits an act of electronic identity theft directly through the use of an unlawful technical means with the intent to derive a benefit or cause harm. (Hijazi, 2021) They are held liable for their criminal conduct under the general law of fraud, forgery and unauthorized access to electronic systems. (Iraqi Penal Code, No.111, 2018)

Liability of the Accomplice and Participant

There is a potential for the involvement of more than one perpetrator when one individual supplies the technical tools and another person performs the hacking or uses stolen information (Hosni, 2019). An accomplice becomes criminally liable when the elements of criminal participation are satisfied, such as agreement, incitement or assistance. (Iraqi Penal Code)

Liability of Educational Institutions

The liability of the educational institution may be triggered in the event of failing to provide proper technical protection of the electronic platform or to protect users' academic information. (OECD, 2022)

The researcher stresses the need to compel educational institutions to adopt modern digital verification systems and effective cybersecurity measures to cut electronic identity theft crimes (Edwards, 2020).

The researcher claims that the task of an educational institution is not restricted to creating digital platforms. It now covers the duty to put in place measures in both the technical and legal aspects of digital identity protection for students, faculty and users. The provisions of the Iraqi Electronic Signature and Electronic Transactions Law No. (78) of 2012, especially the data protection provision and the provision related to electronic transactions. These include adopting 2 factor systems of authentication, electronic signatures, and digital biometrics, and creating special units of cybersecurity within universities to detect suspect activity and respond quickly to hacking and electronic identity theft. (Russel and Norvig, 2021)

Comparative Judicial Applications:

The practice of judges in other countries has revealed an increasing awareness of the gravity of electronic identity theft offenses, and a need for efficient criminal protection of digital identity. (Article 8 of the European Convention on Human Rights).

Certain Egyptian courts have ruled on electronic account ownership and creation and used them in online fraudulent activities under the provisions of Information Technology Crimes Law No. (175) of 2018. Likewise, the U.S. judiciary has been adamant about strict action against online fraud and impersonation in electronic examinations, especially since the increase in distance learning during the COVID-19 pandemic. In the European arena,

some rulings have highlighted the need for safeguarding personal information and digital identity as a component of the right to informational privacy. The Egyptian Anti-Cyber and Information Technology Crimes law No. 175 of 2018)

Conclusion

The study has shown that identity theft crimes in e-learning are one of the most serious crimes in today's cyber-crime landscape because of the impact they have on the integrity of the e-learning process and the security of academic data. It also found a relative lack in the Iraqi legislation as to the regulation of cybercrimes, and the identity theft crime in particular, when compared with Egyptian legislation. In addition to strengthening international cooperation in combating cybercrime, the study underscores the need to create legislative framework for cybercrime, and to update technical and legal protection mechanisms for e-learning platforms. Through the comparative analysis, it becomes clear that rapid technological development necessitates a reconsideration of traditional concepts of criminal protection, as conventional penal provisions are no longer sufficient to address modern digital crimes. This requires the adoption of a specialized digital criminal policy that balances the protection of digital rights and freedoms with ensuring the security of electronic educational institutions. (Edwards, 2020)

Findings

1. The increase in identity theft crimes due to the widespread adoption of e-learning.
2. The insufficiency of Iraqi legislation in comprehensively regulating cybercrimes.
3. The relative superiority of Egyptian legislation in the field of cybercrime control.
4. Weak legal protection for digital educational platforms.
5. The importance of digital evidence and technical expertise in proving cybercrimes.
6. The need to strengthen international cooperation in combating cybercrime.

Recommendations

1. It is recommended to enact a comprehensive Iraqi law to combat cybercrimes.
2. Identity theft in e-learning environments should be explicitly criminalized in texts.
3. Strengthen penalties for attacks on digital educational platforms.
4. Adopt digital verification and electronic authentication methods within universities.
5. Establish specialized cybersecurity units within educational institutions.
6. Enhance international cooperation and information exchange regarding cybercrimes.
7. Train judges and public prosecutors in handling digital evidence.

References

Afifi, A. K. (2000). *Jarayim al-computer* [cybercrimes]. Cairo, Egypt: Dar Al-Nahda Al-Arabiyya.

Al-Hadithi, F. A. R. (2010). *Sharh qanun al-uqubat: Al-qism al-'aam* [Explanation of the penal code: General section]. Baghdad, Iraq: Al-Sanhouri Library.

Al-Kahwaji, A. A. (2002). *Sharh qanun al-uqubat* [Explanation of the penal code]. Beirut, Lebanon: Manshurat Al-Halabi Al-Huquqiyya.

Al-Karbasi, A. M. I. (2000). *Qanun al-uqubat al-iraqi al-nafidh* [The Iraqi Penal Code in force]. Baghdad, Iraq: Al-Zaman Press.

Al-Mudhaki, H. R. (2014). *Al-jarayim al-ma'lumatia* [Information crimes]. Beirut, Lebanon: Manshurat Al-Halabi Al-Huquqiyya.

Al-Zoughbi, J. M., & Al-Mana'isa, O. (2012). *Jarayim taqniyat nuzum al-ma'lumat al-iliktroniya* [Crimes of electronic information systems technology]. Amman, Jordan: Dar Al-Thaqafa.

Barfield, W., & Pagallo, U. (2020). Advanced introduction to law and artificial intelligence. Edward Elgar Publishing.

Challenges of Applying E-Learning in the Libyan Higher Education System.

European Convention on Cybercrime. (2001). *Budapest Convention on Cybercrime*.

EduCTX: A blockchain-based higher education credit platform.

Edwards, L. (2020). Regulating AI in Europe. *European Law Journal*, vol. 25.

Egypt. (2004). *Electronic Signature Law No*. 15 of 2004.

Egypt. (2018). *Law No. 175 of 2018 on Anti-Cyber and Information Technology* Crimes.

Hijazi, A. F. B. (2005). *Al-daleel al-jina'i fi jarayim al-computer wal-internet* [The criminal guide in computer and internet crimes]. Alexandria, Egypt: Dar Al-Fikr Al-Jami'i.

Hijazi, A. F. B. (2019). *Al-jarayim al-iliktroniya wa himayatuha al-qanuniyya* [Electronic crimes and their legal protection]. Alexandria, Egypt: Dar Al-Fikr Al-Jami'i.

Hosni, M. N. (2019). *Sharh qanun al-uqubat: Al-qism al-'aam* [Explanation of the penal code: General section]. Cairo, Egypt: Dar Al-Nahda Al-Arabiyya.

How Unique and Traceable are Usernames?

Iraq. (1969). *Iraqi Penal Code No*. 111 of 1969.

Iraq. (2012). *Electronic Signature and Electronic Transactions Law* No. 78 of 2012.

Khalaf, S. K. (2021). *Criminal protection of e-learning platforms* [Al-himaya al-jina'iyya limansat al-ta'lim al-iliktroni]. (Master's thesis). Al-Nahrain University, Baghdad, Iraq.

Mahmoud, D. K. (2002). Al-Basit fi sharh qanun al-'uqubat: Al-qism al-'amm [The concise explanation of the penal code: General part]. Higher Education Press.

Mansour, M. H. (2018). *Al-himaya al-qanuniyya lil-mawaqi' al-iliktroniya* [Legal protection of websites]. Alexandria, Egypt: New University House.

Nahi, A. D. (2022). Electronic impersonation crimes (comparative study) [Jarayim intihal al-sifa aw al-shakhsiya abr al-wasail al-iliktroniya]. *Maysan Journal for Comparative Legal Studies*, (13), 1–?.

Russell, S., & Norvig, P. (2021). *Artificial intelligence*: A modern approach (4th ed.). Pearson.

Sorour, A. F. (1991). *Al-Wasit fi sharh qanun al-uqubat* [The mediator in explaining the penal code]. Cairo, Egypt: Dar Al-Nahda Al-Arabiyya.

United Nations. (2000). *United Nations Convention against Transnational Organized Crime.*