Interdisciplinary Studies in Society, Law, and Politics 2023; 2(3): 27-36

ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Iran's Legislative Criminal Policy on Cyber Espionage

Seyed Amir. Hashemi[1*], Saeid. Atazadeh[2], Mahmud. Ghayomzadeh[3]

[1] PhD Student, Department of Criminal Law and Criminology, Narag Branch, Islamic Azad University, Narag, Iran
[2] Associate Professor, Department of Criminal Law and Criminology, NAJA Institute of Law Enforcement Sciences and Social Studies, Tehran, Iran
[3] Professor, Department of Education and Law, Saveh Branch, Islamic Azad University, Saveh, Iran

*** Corresponding author email address**: saeidbahjat@yahoo.com

Received: 2023-04-09 **Revised:** 2023-06-14 **Accepted:** 2023-06-24 **Published:** 2023-07-01

Cyber espionage is one of the most prevalent cyber activities. In a simple interpretation and at first glance, cyber espionage appears to be the same as traditional espionage, merely occurring in cyberspace. From this perspective, cyber espionage does not warrant separate recognition, as it inherently falls within the broader framework of espionage. Although this claim may seem valid, it must be acknowledged that cyber espionage is presumed to be novel and distinct from traditional espionage. Therefore, an entity possessing the dual characteristics of novelty (relative to the physical environment) and differentiation (from espionage itself) necessitates separate recognition. The present study is applied in nature and employs a descriptive-analytical method. Data collection was conducted through library research, analyzing books, articles, documents, and codified sources. The findings indicate that the Electronic Commerce Law does not account for instances in which trade secret espionage threatens national security and harms national interests. Therefore, in the modern form of espionage, trade secrets must be distinguished accordingly. In cases where the subject of the crime constitutes both a trade secret and classified data, thereby jeopardizing national security and national interests, prosecution is exclusively governed by the Computer Crimes Law. However, if the perpetrator's act solely involves trade secrets without endangering national security or national interests, it falls under Article 75 of the Electronic Commerce Law and is punishable accordingly. Consequently, traditional methods of detection, prosecution, investigation, and prevention are no longer effective for addressing this crime. The development and coordination of countermeasures against cyber espionage require tools and expertise commensurate with the offenders operating in this domain.

Keywords: *Legislative criminal policy, espionage, cyberspace, crimes against security*

How to cite this article:

Hashemi, S. A., Atazadeh, S., & Ghayomzadeh, M. (2023). Iran's Legislative Criminal Policy on Cyber Espionage. *Interdisciplinary Studies in Society, Law, and Politics, 2*(3), 27-36. https://doi.org/10.61838/kman.isslp.2.3.4

1. Introduction

In a general definition, computer or cyber espionage refers to the "unauthorized search to examine the status of computer targets, assess a computer defense system, view information, or illegally copy data files" (CRS, 2008, p. 12). Cyber espionage includes unauthorized surveillance to discover the configuration of a targeted computer, assess its security protections, or unlawfully browse and copy data files.

Cyber espionage is among the most prevalent cyber activities, whether it is used to expose sensitive governmental information, steal trade secrets and commercial data, or as part of intelligence and reconnaissance operations. More precisely, espionage, from a doctrinal perspective, falls within the framework of using informational superiority to

achieve significant victories at a lower cost (Abrar Moaser Tehran International Cultural Studies Research Institute, 2012a, 2012b).

Cyber espionage is one of the most recent and significant forms of crimes against security, occurring through computer and telecommunication systems. Consequently, traditional methods of detection, prosecution, investigation, and prevention are no longer effective in addressing this crime. Developing and coordinating countermeasures against cyber espionage require tools and expertise equivalent to those possessed by offenders in this domain (Farhadi Alashti, 2011).

The novelty of cyber espionage stems from the new medium in which it is committed. However, its distinction from traditional espionage lies in differences in certain conditions and material elements of the crime, or more precisely, in the blameworthy conduct itself. Otherwise, cyber espionage is not an entirely separate phenomenon but rather a modern manifestation of espionage itself.

2. Definition of the Crime of Espionage:

Some legal scholars define "espionage" as the collection and acquisition of information and instructions or documents usable by a foreign country against the security of another foreign country (Garo, 1964, Vol. 3, p. 12). In legal terminology, espionage refers to the gathering of secret and classified information regarding offensive and defensive operations, obtaining intelligence on political or economic conditions, scientific and industrial secrets, and military affairs of a nation, with the intent of providing them to unauthorized individuals or foreign entities in exchange for any form of compensation or gratuitously, in alignment with enemy objectives. This process aims to identify a nation's strengths and weaknesses to block avenues for empowerment and exploit vulnerabilities for destructive purposes (Mortazavi, 2006).

It is important to note that this definition is neither comprehensive nor exclusive, as it criminalizes only the espionage of trade and industrial secrets while neglecting other forms of classified information that have security implications. Additionally, the intent and motive of the perpetrator are limited to economic harm or financial gain, whereas an individual engaging in espionage may have other objectives as well.

Based on the discussions presented, a proposed definition of computer espionage is: unauthorized and intentional surveillance, access, and disclosure of valuable electronic messages and information, including commercial, political, military, cultural, and security-related data, conducted in cyberspace with the aim of harming natural or legal persons, whether in the private or public sector.

Espionage, in its broadest sense, encompasses two categories of actions. The first includes preparatory actions, such as investigating and obtaining secret information, while the second consists of operational activities, including establishing communication and transmitting the gathered information to those intended to exploit it. When the acquisition of confidential information occurs fraudulently in cyberspace and the secrets being spied upon involve confidential computer data or when information is obtained through computers or other electronic means in cyberspace, computer espionage is realized.

3. Examination of the Constitutive Elements of Espionage:

For an act to constitute a crime, certain elements must be present. Some elements are general, while others are specific.

One of the general elements of any crime is its formal recognition as an offense under the law, with an associated punishment prescribed (the legal element) (Sanei, 1992).

This principle is derived from various sources, including verses of the Qur'an, such as "We would not punish until We had sent a Messenger" (Qur'an 17:15), as well as hadiths from the Imams and the rational principle that punishment without prior notification is unjust. This principle is reflected in Latin legal maxims.

In accordance with this principle, valid and enforceable laws criminalizing espionage fall into two categories:

The first category includes laws and regulations that explicitly reference espionage and spies. Among these are Articles 6, 7, and 8 of the Islamic Penal Code (Discretionary Punishments) approved on August 9, 1983, Article 12 of the Penal Code for Armed Forces

Crimes approved on August 9, 1992, and Articles 501, 502, and 510 of the Islamic Penal Code of 1996.

The second category consists of laws and regulations that do not explicitly mention "espionage" or "spies" but can be interpreted as encompassing espionage based on their nature, purpose, and specific conditions. These include Articles 3, 4, 5, and 9 of the Islamic Penal Code (Discretionary Punishments), Article 313 of the Penal Code for Armed Forces Crimes, and Articles 503, 505, and 509 of the Islamic Penal Code of 1996.

Accordingly, the legal framework in the Islamic Republic of Iran criminalizes espionage, and its legal element is established through the aforementioned legal provisions.

In modern criminal justice systems, individuals are not prosecuted or punished solely based on their criminal thoughts. Therefore, one of the essential elements of a crime is its material element (actus reus), meaning that criminal intent alone is insufficient to constitute a crime. There must be an act or conduct, accompanied by mens rea (criminal intent), that is recognized by law as a crime. Consequently, a mere criminal intent without an accompanying criminal act generally does not constitute a crime.

To establish the material element of a crime, there must be an unlawful reaction against legal norms and regulations. This reaction may take different forms, including acts of omission. Legal scholars categorize the material element into the following forms (Sarikhani, 2016):

1. Commission (positive act);
2. Omission (failure to act);
3. Commission by omission;
4. Possession and retention;
5. Status or condition.

Based on the relevant legal provisions, the material element of espionage is characterized by a positive act, meaning that omission or an act of commission by omission does not constitute espionage.

In addition to the legal and material elements, the mental element (mens rea) is also necessary for the commission of a crime. The mere occurrence of a criminal act does not automatically imply the presence of mens rea. In some cases, even when a criminal act is committed, the law does not impose punishment due to the absence of criminal intent or liability.

For the mental element to be established, two factors must be present:

1. The will to commit the act (i.e., the person must intend to carry out the criminal act);
2. Criminal intent (i.e., the intent to unlawfully use the obtained information).

Thus, merely committing an act of intelligence gathering does not constitute espionage unless there is an accompanying criminal intent. If the act of surveillance and data collection is done voluntarily but without an intent to unlawfully exploit the information, the crime of espionage is not established. Therefore, espionage, as defined in law, requires both general intent (awareness and willingness to commit the act) and specific intent (the purpose of using the obtained information for unauthorized purposes). The act itself is typically detrimental to national security, the nation, and the government, as classified documents and confidential information remain valuable only as long as they are inaccessible to unauthorized individuals. Once criminal actors gain access through illegal means, the damage to national interests becomes inevitable.

From the above discussion, it is evident that espionage is an intentional crime. However, in some cases, the perpetrator may commit the act voluntarily without intending its criminal consequences or may fail to foresee the resulting harm. In such cases, the mental element is considered to arise from criminal negligence, rendering the act involuntary espionage (Sarikhani, 1999).

4. The Crime of Espionage in the Islamic Penal Code

This section examines the constitutive elements of the crime of espionage under the Islamic Penal Code.

4.1. The Legal Element of Espionage

Since Articles 501, 502, 503, and 510 of the Islamic Penal Code employ the general term "whoever," the crime of espionage applies to civilians, regardless of their nationality (Iranian or foreign), religion (Muslim or non-Muslim), or employment status (government employee or non-government employee).

Article 501: "Whoever knowingly and deliberately provides maps, secrets, documents, or decisions related to the country's domestic or foreign policies to unauthorized individuals or informs them in a manner that constitutes espionage shall be sentenced, depending on the nature and degree of the crime, to imprisonment ranging from one to ten years" (Khodagholi, 2004).

Article 502: "Whoever commits an act of espionage in favor of a foreign state and to the detriment of another foreign state within the territory of Iran, in a manner that harms national security, shall be sentenced to imprisonment ranging from one to five years."

4.2. The Material Element of Espionage

Under Articles 501 and 502, espionage can be committed by any individual, whether Iranian or foreign, Muslim or non-Muslim, government employee or otherwise, who obtains secrets by any means. These secrets may include maps, documents, and decisions related to military installations, fortifications, or bases, as well as non-military maps that are prohibited from public disclosure. If such information is provided to unauthorized individuals, the crime is established.

The offender must have positively engaged in a material act, first by knowingly and deliberately acquiring secrets that were legally prohibited from their knowledge, and then by knowingly and deliberately transferring these classified secrets to others.

This crime does not differentiate between the full or partial disclosure of secrets, nor does it distinguish between oral and written disclosure.

Article 503: "Whoever, with the intent of theft, mapping, or obtaining information on political, military, or security secrets, enters relevant locations, as well as any person who is apprehended while mapping, filming, or photographing military fortifications or restricted areas without authorization from competent officials, shall be sentenced to imprisonment ranging from six months to three years."

In this article, the material act committed by the offender consists of:

1. Entering locations where secrets and documents are stored with the intent to steal.
2. Entering such locations with the intent to conduct mapping.
3. Engaging in mapping, filming, or photographing military fortifications or restricted areas.

Article 510: "Whoever, with the intent of disrupting national security or aiding the enemy, knowingly conceals spies assigned to conduct reconnaissance or inflict harm on the country, or facilitates their concealment, shall be sentenced to imprisonment ranging from six months to three years."

The material act in this case is the concealment of spies, constituting a positive material act.

4.3. The Mental Element of Espionage

Espionage is an intentional crime, and its commission requires the offender's criminal intent. The perpetrator must knowingly and deliberately engage in espionage, fully aware that the disclosed information is classified and pertains to significant military, political, economic, industrial, or scientific matters, including encryption keys (Khodagholi, 2004). Despite this knowledge and malicious intent, the offender acquires the secrets and transfers them to another party, fully aware that such disclosure harms national interests.

The court must establish criminal intent. If the disclosure of secrets results from ignorance, mistake, negligence, or coercion, the mental element of the crime is undermined, and the act does not constitute espionage. Espionage may be committed directly or indirectly, but this distinction does not affect its legal classification.

5. Examination of Laws and Elements Related to Cyber Espionage

This section analyzes the constitutive elements of cyber espionage under the Computer Crimes Law.

5.1. The Legal Element of Cyber Espionage

The Computer Crimes Law classifies cyber espionage into several categories:

1. Unauthorized access to computer and telecommunication systems storing classified data (Article 4 of the Computer Crimes Law).

2. Accessing, obtaining, or intercepting classified data (Clause A of Article 3 of the Computer Crimes Law).
3. Making classified data available to unauthorized individuals (Clause B of Article 3 of the Computer Crimes Law).
4. Providing classified data or disclosing it to foreign governments, organizations, companies, or their agents (Clause C of Article 3 of the Computer Crimes Law).
5. Negligence or recklessness by government officials in handling classified information (Article 5 of the Computer Crimes Law).

The first category refers to unauthorized access to systems containing classified data, while the second category involves unauthorized access to the classified data itself. Both constitute the offense of unauthorized access, with interception added as an aggravating factor. Thus, unauthorized access and illegal interception serve as the foundation of cyber espionage.

Article 3 of the Computer Crimes Law states:

"Whoever, without authorization, engages in the following acts concerning classified data in transit, stored in computer or telecommunication systems, or on data carriers, shall be subject to the prescribed penalties:"

A) Accessing or obtaining such data or intercepting its classified content in transit shall be punishable by imprisonment ranging from one to three years or a fine between 20,000,000 to 60,000,000 rials, or both.

B) Making such data available to unauthorized persons shall be punishable by imprisonment ranging from two to ten years.

C) Disclosing or making such data available to a foreign government, organization, company, or its agents shall be punishable by imprisonment ranging from five to fifteen years.

5.2. The Material Element of the Crime of Espionage in Cyberspace

The material element of this crime generally consists of the commission of certain unauthorized acts, as described in Clauses A, B, and C of Article 3 of the Computer Crimes Law, involving classified data that is in transit or stored in computer systems, telecommunication networks, or data carriers.

Under Clause A of Article 3, the criminal acts include:

1. Accessing classified data
2. Obtaining classified data
3. Intercepting classified content in transit

To clarify the meaning of this clause, it is essential to recognize that espionage, in its broadest sense, encompasses two categories of actions. The first category includes preparatory actions, such as investigating and obtaining confidential information. The second category consists of executive operations, involving establishing communication and transmitting the obtained information to unauthorized individuals for exploitation. The first category may not necessarily indicate an intent to commit espionage or treason. For instance, a suspect may have acted out of mere curiosity, a desire for knowledge, negligence, or recklessness, or may have acquired confidential information solely to inform the public rather than foreign entities. However, the second category always reveals a specific intent to inform unauthorized and unqualified entities (Goldouzian, 2003a, 2003b).

The structure of Clause A, along with certain indications—such as the lack of any explicit requirement that unauthorized acts involve the transfer of information to unqualified individuals—suggests that the acts mentioned in Clause A fall within the category of preparatory actions. Therefore, if there is no clear evidence of espionage, the mere commission of these acts cannot be classified as espionage. What criminalizes accessing, obtaining, or intercepting classified content is their unauthorized nature. Thus, it would have been more appropriate for the term "unauthorized" to be placed at the beginning of this clause rather than at the start of the article.

The term "access" linguistically refers to power, ability, or the capability to reach something (Amid, 2008, p. 34). Accordingly, an individual who gains unauthorized access to classified data does so independently, without seeking assistance from others. For example, the individual hacks into a system to collect the data. This differs from obtaining classified data, where the offender initially lacks direct access to the information but acquires it through interaction with someone who possesses it. The linguistic definition of "obtaining" supports this

interpretation, as the term means "to acquire or procure" (Moin, 1983).

Next, we will analyze the material elements of Clauses A, B, and C of Article 3 of the Computer Crimes Law separately:

Under Clause A of Article 3, the criminal acts include:

1. Accessing classified data
2. Obtaining classified data
3. Intercepting classified content in transit

To understand this clause, it is crucial to note that espionage in its broad sense includes two categories of actions: preparatory actions, such as investigating and obtaining confidential information, and executive operations, which involve establishing communication and transmitting the obtained information to unauthorized individuals. The first category may not necessarily imply an intent to commit espionage or betrayal. For example, a suspect may have acted out of curiosity, a desire for knowledge, negligence, or recklessness, or may have obtained classified information with the intention of informing the public rather than foreign entities. However, the second category always demonstrates a deliberate intent to provide information to unauthorized entities.

The structure of Clause A, along with certain indicators—such as the absence of a requirement that unauthorized acts involve the transfer of classified information—suggests that the acts described fall within the category of preparatory actions. This means that if no clear evidence of espionage exists, merely committing these acts cannot be considered espionage. What criminalizes accessing, obtaining, or intercepting classified content is their unauthorized nature. Thus, it would have been preferable for the term "unauthorized" to be placed at the beginning of this clause instead of at the start of the article.

The term "interception" refers to covertly listening to the conversations of others (Sarikhani, 2016), and in this context, it applies to classified content in transit. However, unauthorized interception of non-classified content is separately criminalized under Article 2 of the Computer Crimes Law. According to this article:

"Whoever unlawfully intercepts non-public communications in transit through computer or telecommunication systems, electromagnetic waves, or optical signals shall be sentenced to imprisonment ranging from six months to two years or a fine between 10,000,000 to 40,000,000 rials, or both."

The crime under Clause A of Article 3 is a result-based offense, meaning that for it to be considered committed, the offender's actions—whether accessing, obtaining, or intercepting classified data—must successfully result in acquiring such data. If the offender fails to obtain classified data, their act may fall under Article 4 of the same law.

In Clause B of Article 3, the law explicitly emphasizes "making classified data available," which logically implies that such data—whether in the form of videos, photographs, texts, etc.—must be directly provided to an unauthorized person. The mere disclosure of the contents of such data, which is an indirect means of making it available, is not covered by this clause and does not constitute a crime. If the legislator intended to criminalize "making the contents of classified data available," it would have used terminology similar to Article 501 of the Islamic Penal Code, which explicitly includes "content" in its definition of espionage. Thus, one of the deficiencies of Clause B of Article 3 is its failure to distinguish between providing the actual data and revealing its contents. Given the high sensitivity and importance of classified data, there is no logical distinction between providing the data itself and disclosing its content, as unauthorized access to either harms national security (Mir Mohammad Sadeghi, 2017, p. 85).

However, disclosing the contents of classified data may still be considered a crime under Article 501 of the Islamic Penal Code. If the data contains maps, secrets, documents, or decisions related to the country's domestic or foreign policies, disclosing its content to unauthorized individuals constitutes espionage. Nonetheless, to eliminate ambiguities, the legislator should have explicitly included "content" in this clause.

Regarding Clause C of Article 3, criminal law does not provide a specific definition of "disclosure." However, according to Article 19 of the Regulations on the Protection of Classified Military Documents and Information, enacted in 1996 by the General Staff of the Armed Forces, "disclosure" is defined as:

"The act of presenting the content of classified documents or information, whether verbally, in writing,

or through any other means that compromises its security and confidentiality."

The distinction between "disclosure" and "making data available" lies in their nature. An act is considered "disclosure" when the offender personally provides the classified data to another party. In contrast, "making data available" is a passive act, where the offender facilitates access without directly handing over the information. For instance, if an offender deliberately provides their computer password to a foreign agent, who then accesses and retrieves classified data, the act constitutes "making data available" rather than "disclosure."

Regarding the term "foreign," which is generally applied to non-citizens, there is no ambiguity when it qualifies governments, organizations, companies, or groups, as it clearly refers to non-Iranian entities. However, in the case of agents of such entities, a question arises: Must the agent also be a foreign national? Given that espionage operations often involve local agents recruited by foreign states, the correct interpretation is that an Iranian citizen can also be an agent of a foreign entity. Therefore, disclosing or making classified data available to such an Iranian agent also falls within the scope of Clause C of Article 3 and does not require the agent to be a foreign national.

5.3. *The Mental Element of Espionage*

For the mental element to be established, two factors must be present:

1. The will to commit the act (i.e., the individual must intend to perform the criminal act).
2. Criminal intent.

Therefore, the will to commit an act without criminal intent does not constitute a crime. If an individual intentionally gathers intelligence but lacks the criminal intent (i.e., there is no intention to use the information unlawfully), the crime of espionage is not established. Thus, in addition to conducting intelligence gathering, criminal intent must be proven for cases of intentional espionage, while in cases of unintentional espionage, criminal negligence must be established.

Accordingly, considering the legal definition of espionage, the mental element comprises general and specific intent—meaning the deliberate intent to engage in espionage despite legal prohibitions, with the act typically causing harm to the country, nation, or government. Classified and confidential documents remain valuable as long as unauthorized individuals do not gain access to them. Once criminal actors obtain them through illegal means, damage to the country becomes inevitable.

From the above discussion, it is clear that espionage is an intentional crime. However, in some cases, the offender may commit the act voluntarily but not intend the criminal outcome or fail to foresee the consequences of espionage. In such cases, according to legal scholars, the mental element of the crime arises from negligence, and the offense is considered unintentional espionage (Sarikhani, 2016).

As previously mentioned, espionage is an intentional crime, and its commission requires the offender's criminal intent. The offender must knowingly and deliberately engage in espionage, being fully aware that the information is classified and includes sensitive military, political, economic, industrial, scientific matters, or encryption keys (Khodagholi, 2004). Despite this awareness, the offender, with full knowledge and criminal intent, transfers the classified information to another party, knowing that its disclosure harms national interests.

In cases of espionage, the court must determine the presence of criminal intent. If the disclosure of secrets results from ignorance, mistake, negligence, or coercion, the mental element is weakened, and the act does not constitute espionage. Espionage may be committed directly or indirectly, but this distinction does not affect the legal classification of the offense.

Regarding cyber espionage, Article 3 of the Computer Crimes Law states:

"Whoever unlawfully commits the following acts concerning classified data in transit or stored in computer or telecommunication systems or data carriers shall be subject to the prescribed penalties:"

A) *Accessing or obtaining such data or intercepting its classified content in transit shall be punishable by imprisonment ranging from one to three years or a fine between 20,000,000 to 60,000,000 rials, or both.*

B) *Making such data available to unauthorized persons shall be punishable by imprisonment ranging from two to ten years.*

C) *Disclosing or making such data available to a foreign government, organization, company, or its agents shall be punishable by imprisonment ranging from five to fifteen years.*

The material element of this crime generally consists of committing unauthorized acts, as described in Clauses A, B, and C, concerning classified data in transit or stored in computer or telecommunication systems or data carriers.

5.3.1. *Examination of the Mental Element in Clause A of Article 3*

The mental element of the offense in Clause A consists of intentional acts of accessing, obtaining, or intercepting classified content, as well as knowledge and awareness that the access, acquisition, or interception is unauthorized and without proper authorization. Additionally, the offender must be aware that the data is classified. Thus, if an individual mistakenly believes that the data is ordinary, they do not commit this crime.

5.3.2. *Examination of the Mental Element in Clause B of Article 3*

The mental element of this offense consists of intentionally making classified data available. Therefore, if an individual commits the act while intoxicated, unconscious, asleep, under duress, or coercion, they do not fall under this clause. Furthermore, the offender must be aware that the data is classified and that the recipient is unauthorized. However, specific criminal intent—such as intending to harm national security or disrupt the country's stability—is not required.

5.3.3. *Examination of the Mental Element in Clause C of Article 3*

The mental element of the offense in Clause C consists of intentionally disclosing or making classified data available, as well as awareness that the recipient is a foreign entity, which may include a government, organization, or company.

Moreover, specific criminal intent—such as intending to undermine national security or harm the country's political or military stability—is not required. The mere act of disclosing or making classified data available is sufficient to constitute espionage under this clause.

5.3.4. *Negligence and Recklessness in Protecting Classified Data*

Espionage is typically classified as an intentional crime, as the offender, with criminal intent, transfers classified information to foreign entities or unauthorized individuals. However, due to the critical importance of safeguarding classified information and the potential harm caused by negligence or failure to protect it, legislators have criminalized such negligence under Article 506 of the Islamic Penal Code.

Similarly, Article 5 of the Computer Crimes Law addresses negligence in safeguarding classified data, but it is specifically adapted to technological advancements. Unlike Article 506, which does not specify particular classifications of information, Article 5 explicitly criminalizes negligence in handling classified data.

According to Article 5 of the Computer Crimes Law:

"If government officials responsible for protecting classified data, as specified in Article 3 of this law, or related systems—having received the necessary training or having been entrusted with such data or systems—through negligence, recklessness, or failure to observe security protocols, allow unauthorized individuals to access such data, data carriers, or systems, they shall be sentenced to imprisonment ranging from ninety-one days to two years or a fine between 5,000,000 to 40,000,000 rials, or both, along with dismissal from service for a period of six months to two years."

Negligence typically involves performing an act that should not be done. For example, if an official leaves a data carrier unattended on their desk and someone enters the room and takes it, this constitutes negligence. Recklessness, on the other hand, refers to failing to take necessary precautions, such as failing to password-protect a computer, thereby allowing unauthorized individuals to access confidential information simply by turning it on (Mir Mohammad Sadeghi, 2017, p. 97).

It is essential to note that, although this offense is not an intentional crime, negligence, recklessness, and failure to observe security measures must be proven.

Thus, if an official, due to torture, forced intoxication, or while asleep, transfers classified data to unauthorized individuals, they are not liable under this article.

Another important consideration is that negligence and recklessness may apply to two aspects:

1. Failure to protect classified data itself (e.g., leaving classified documents unattended).
2. Failure to verify the identity of the recipient (e.g., assuming an individual is authorized based on their claim and providing them access to classified data without proper verification).

6. Conclusion

In comparing cyber espionage with traditional espionage, the most evident necessity is the requirement for proper legislation regarding cyber espionage. Although espionage can occur through various means, for instance, by conveying information via telephone to another natural or legal person, and the medium used does not alter the nature of the crime, cyber espionage differs in certain respects. These differences distinguish it from traditional espionage and shape it into a modernized form of the crime.

For example, in general espionage laws, it has been established that punishments differ between military and non-military offenders. This raises the question: With the increasing digitization of all affairs, if a military personnel gains access to security-related matters through a computer and transfers them—whether using a computer or another method—should they be subject to Hadd (fixed punishment under Islamic law) or Ta'zir (discretionary punishment)? In this scenario, the computer is utilized for obtaining the information, but the transfer may or may not involve a computer. Conversely, should there still be a distinction between military and non-military personnel when committing cyber espionage? These are questions that lawmakers must address.

Regarding cyber espionage, it is clear that existing laws are inadequate. For example, Articles 501 and 502 of the Islamic Penal Code are applicable to ordinary offenders of this crime. However, a brief analysis reveals the shortcomings of these laws in addressing the specific and modern nature of cyber espionage and its unique elements.

As many countries have enacted specialized laws regarding computer crimes, the need for such legislation in Iran is increasingly evident. This necessity is particularly pressing given that traditional espionage laws in Iran are primarily focused on military, political, and national security issues, overlooking commercial and economic espionage. In contrast, many countries have explicitly criminalized economic espionage, recognizing its significance in the digital age.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

Not applicable.

References

Abrar Moaser Tehran International Cultural Studies Research Institute. (2012a). *Security and cyber warfare, special on cyber laws*. Abrar Moaser Tehran International Cultural Studies and Research Institute.

Abrar Moaser Tehran International Cultural Studies Research Institute. (2012b). *Security and cyber warfare, special on weapons, warriors and cyber attacks*. Abrar Moaser Tehran International Cultural Studies and Research Institute.

Farhadi Alashti, Z. A. U. J. J. B. A. (2011). Challenges facing situational prevention of transnational cyber crimes. *Intelligence and Criminal Research Quarterly*, *12*(1).

Goldouzian, I. (2003a). *Annotated Islamic penal code*. Majd Scientific and Cultural Complex.

Goldouzian, I. (2003b). *Specific criminal law*. University of Tehran Publications.

Khodagholi, Z. (2004). *Computer crimes*. Arian Publications.

Moin, M. (1983). *Persian dictionary, Vol. 4*. Amirkabir Publications.

Mortazavi, S. (2006). *Crimes against security and public welfare*. Majd.

Sanei, P. (1992). *General criminal law* (Vol. 1). Ganj-e Danesh.

Sarikhani, A. (1999). *Espionage and treason*. Islamic Propaganda Office Publications Center.

Sarikhani, A. (2016). The position of eavesdropping in violation of privacy from the perspective of jurisprudence and law; A reflection on the book "Examining the jurisprudential and legal rulings of eavesdropping". *Journal of Jurisprudence and Law*, *5*.