Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 15 (02), 2023
pp. 460 - 473

Analyzing the dimensions and components of criminal protection of classified data in computer space

Mehdi Abdi

Abstract

Classified data is considered a vital asset in the security, economic and social fields, and any attack on it can cause heavy losses. Computer space, with its features such as transnationality and anonymity, has paved the way for committing crimes against this data. In fact, the main concern of this research is to answer the question of to what extent the Iranian criminal law system has been able to effectively protect classified data in computer space by utilizing substantive and formal regulations? The present study was conducted using a descriptive-analytical method with the aim of explaining and analyzing the substantive and formal dimensions of criminal protection of classified data in the computer space and providing legal and legislative solutions to improve the efficiency of the Iranian criminal system in this area. Based on the findings of the study, although Iranian criminal law has covered some of the threats through criminalization and the provision of formal mechanisms, it still faces legislative gaps, implementation challenges, and weaknesses in judicial mechanisms that prevent the full realization of criminal protection. Therefore, reviewing existing laws, utilizing the experiences of other countries, and further compliance with international documents can be an effective step in ensuring the security of classified data.

Keywords: Classified data, criminal protection, computer crimes, Iranian criminal law

Received: 20/10/2023 **Accepted :11/12/2023** **Published: 17/12/2023**

1- Introduction

With the increasing development of information and communication technology, data, especially classified and confidential data, play a key role in the security, economic, social and cultural structures of societies. These data are not only recognized as strategic assets at the national level, but also considered the key to the survival of countries and ensuring global security in the international arena. In such circumstances, cyberspace, with its unique features such as transnationality, anonymity of users, permeability and high speed of data exchange, has provided a new arena for countless threats against these vital assets. Committing crimes such as unauthorized access, interception of sensitive information, cyber espionage, computer forgery and data destruction not only endangers the fundamental rights of individuals and their privacy, but also threatens national security and weakens the country's economic system. From this perspective, the fundamental question is how and to what extent the Iranian criminal law system has been able to provide a basis for effective protection of classified data in the computer space by utilizing substantive and formal regulations.

Now, the main question is, “To what extent has the Iranian criminal law system been able to provide effective protection of classified data in the computer space by utilizing substantive and formal regulations?” The answer to this question, presented in the form of the main hypothesis, is: “It seems that Iran’s criminal regulations in the field of protecting classified data in the computer space, while criminalizing some threats and predicting some formal mechanisms, are still faced with legislative gaps and executive challenges that prevent the full realization of criminal protection.” This connection between

the question and the hypothesis shows that the issue is not only theoretical but also a practical and applicable concern for the country's criminal policymaking.

The present study aims to "explain and analyze the substantive and formal dimensions of criminal protection of classified data in the computer space and provide legal and legislative solutions to improve the efficiency of the Iranian criminal system." To achieve this goal, a descriptive-analytical research method has been chosen, which is based on documentary analysis, comparative study, and examination of domestic and international experiences. This method allows for the identification of the weaknesses and strengths of existing laws, while examining the theoretical dimensions and legal foundations of the subject, and for practical solutions to be provided based on them. The necessity of conducting this study is important in several aspects: First, with the increase in cyber threats, classified data has been exposed to more danger than ever before, and any lack of coherent criminal protection has serious consequences for national security, social order, and public trust. Second, although important steps have been taken in the criminalization of some cybercrimes in Iranian law, weaknesses are observed in the areas of punishment, determination of judicial jurisdiction, development of crime detection mechanisms, and collection of digital evidence. These shortcomings indicate that a comprehensive and all-encompassing study is inevitable to identify challenges and provide scientific and legislative solutions. Third, this research has contributed theoretically to the enrichment of the country's scientific literature and, from a practical perspective, can be useful for improving legislative and judicial policy, especially in institutions such as the judiciary and the FATA police.

A review of previous studies shows that existing research has mostly dealt with computer crimes and cyberspace in general. For example, Masoudi (2011) introduced cyberspace and types of cybercrimes in his work, although the issue of criminal protection of classified data was not specifically raised. Jalali Farahani (2006) and Javanbakht (2009) focused on the issue of criminal jurisdiction in cyberspace and examined the shortcomings in this area. On the other hand, Bastani (2004) addressed computer crimes and related legislative problems, and Foroughi (2009) analyzed the principle of universal jurisdiction in relation to international crimes. In addition, some translated sources, such as the book "International Criminal Law" by Shiazari et al., are primarily devoted to the issue of international criminal justice and war crimes and have no direct connection to the field of cybercrimes. Therefore, the existing literature has either been very general and general or has focused on specific aspects such as jurisdiction and has focused less on the issue of criminal protection of classified data.

The main innovation of this article lies in the specific and simultaneous focus on the substantive and formal dimensions of criminal protection of classified data in the computer space. Unlike previous studies that have mainly limited themselves to introducing cyberspace, types of computer crimes or criminal jurisdictions, this research focuses on confidential and sensitive data and examines how criminalization, punishment and the efficiency of criminal proceedings are carried out in this area. In addition, by analyzing the role of the FATA police, judicial authorities and digital evidence collection mechanisms, the present article presents a comprehensive approach that both theoretically responds to the gaps in the scientific literature and can be a practical guide for policymakers and legislators in the country. It can be said that this research is the first coherent effort in the domestic field that examines the criminal protection of classified data in both substantive and formal dimensions in an integrated manner.

-1Fundamentals and Concepts

-1 -1Definition and Position of Classified Data

One of the comprehensive definitions of classified data is provided by "Fung and Chowhan"; based on this definition, data classification is a systematic process of organizing structured or unstructured data into logical groups, in such a way that the goals of security, compliance with laws, and efficiency in data retrieval are best achieved. In fact, the data classification process determines the priorities related to their protection, maintenance, and dissemination by determining the level of sensitivity and value of each type of data (Fung & Chowhan, 2020, p. 112). For example, in the field of information security, data is divided

into the categories of “public”, “internal”, “confidential” and “top secret”, and each category has its own set of policies, access levels and protection measures (Bertino & Sandhu, 2005, p. 17). Thus, data classification plays a key role in ensuring the security and confidentiality of information, in addition to simplifying data management and statistical analysis.

The place of classified data in data management structures and information security systems plays a central and strategic role. The importance of this data becomes more prominent when a very high volume of data is generated and stored in organizations or information systems. Effective data classification provides transparency in how to deal with types of information, facilitates access based on need, reduces the risk of unwanted disclosure and manages security and storage costs. According to Frantz and Nowklass, data classification and categorization, especially in organizational environments and information systems, is a fundamental tool for implementing data security policies, legal requirements, and protecting user rights; also, implementing efficient classification is itself a prerequisite for realizing big data analytics, machine learning, and artificial intelligence. In addition, organizations that have strong and structured data classification policies have a greater ability to comply with international standards and prevent cyber threats. (Frantz, P. & Nowklass, S, 2017, p. 49)

1 2 -- The concept of information security (confidentiality, integrity and availability)

-1 -2 -1Confidentiality

The concept of confidentiality in information security is not limited to preventing data from being viewed by unauthorized persons; it is also a platform for creating a system of trust, ensuring intellectual property and even respecting human rights in the digital era. The principle of information confidentiality implies that all information architectures must be designed in such a way that data transmission, storage and processing are carried out only by authorized agents. Encryption technologies, multi-factor authentication systems, segmentation of access domains and continuous monitoring are the most important mechanisms that have been proposed in the specialized literature to realize this principle. Although a breach of confidentiality may seemingly only lead to the disclosure of information, on a macro level it will lead to a threat to national security, the emergence of economic and social crises or even the loss of public trust in a system or brand; Therefore, it is always recommended that security policies and processes prioritize data confidentiality first, then integrity protection, and finally availability (Whitman & Mattord, 2017, pp. 21-23).

-2 -2 -1Extensive Integrity Analysis

Integrity is the beating heart of any information system, as it ensures that data is not only protected from unauthorized changes, but also that business processes and strategic decisions are based on correct, complete, and fact-based data. Integrity includes both regular monitoring of data changes, automated validation, and maintaining backups, and also targets organizational culture and professional ethics: if employees or systems can easily change or delete data without being traced, the foundation of trust collapses completely. The role of hash algorithms and digital signatures is important to the extent that even the smallest changes in data can be detected. In addition, the existence of periodic audit checklists, change management, and accurate logging have been introduced as key tools for maintaining integrity (Peltier, 2016, pp. 32-36). In a macro analysis, ignoring the principle of integrity disrupts the order and transparency of information and makes entire data-dependent systems inefficient or even destructive.

-3 -2 -1Availability in the infrastructure and application layers

Accessibility is the most superficial and at the same time the most vital component of the information security model, because even if the most excellent confidentiality and integrity mechanisms are implemented, the lack of access to data and services calls into question the efficiency of the entire system. The scope of this principle includes not only storage systems and servers but also communication networks, cloud services, disaster recovery policies and even human emergency response capabilities. Denial of service attacks, hardware failures, catastrophic events or even human disruptions are all among

the most important threats to availability. Therefore, classical studies emphasize scalable architecture, the presence of alternate servers, real-time monitoring and alerts and the deployment of immediate recovery systems after a crisis. Ignoring this principle leads to delays in service delivery and, as a result, loss of revenue and trust, which in some industries such as healthcare or fintech, costs human lives or billions of rials of national capital (Andress, 2014, pp. 51-54). 3-1- Characteristics of Cyberspace and Its Challenges in Criminal Protection

Cyberspace is distinguished by its features such as borderlessness and translocation, innovative tools, and easy flow of information. In this space, individuals' identities can be easily hidden and data can be accessed on a global and immediate level. The high speed of data transfer, the ability to edit or delete traces, and the ability for users to log in and out instantly are among the most important features of this platform. These features have caused many traditional legal concepts – such as identity verification, determining territorial jurisdiction, and focusing on data ownership – to lose their former effectiveness in cyberspace or to require a substantial revision. In addition, the anonymity and ease of committing crimes make prosecution much more difficult than in the physical environment (Dashti, 2019, p. 7 PDF).

In the Iranian criminal law system, several challenges have emerged in criminal protection of individuals' rights in the face of cybercrimes. The first and most fundamental challenge is the lack of full compliance of domestic laws – especially the Islamic Penal Code and the Computer Crimes Law – with the complexities and continuous developments of cyber technologies. The limitations of the territorial jurisdiction of criminal laws, legal gaps in the criminalization of new crimes such as malware attacks, phishing, privacy violations, and cyber financial crimes, and the inability of investigation and prosecution mechanisms to quickly and effectively identify defendants are among the most important challenges. Despite the addition of articles related to the criminal liability of legal entities in the law, practical implementation and monitoring are very difficult, because identifying unknown criminals and proving their role in the dispersed and changing cyberspace requires mechanisms beyond existing capabilities. The weakness of technical infrastructure, the obvious gap with international standards, and the lack of efficient specialized teams have seriously damaged the investigation process and in many cases led to the criminalization of the perpetrators and the ineffectiveness of the punishment (Yebloui, 2017; 56). One of the important gaps in criminal protection is related to the procedural rules and the identification of challenges that arise in the process of collecting electronic evidence, determining the jurisdiction of the courts, and preserving the guaranteed rights of the accused and suspects. The current laws of Iran are largely unresponsive to the innovative methods of committing crimes, the scope of concealment techniques, and the deconstruction of identity in cyberspace, and these deficiencies undermine the acceptance and implementation of criminal justice. According to scientific studies, even new criminalizations in the law of computer crimes are mainly based on classic patterns and are incompatible with the challenges of cyberspace, and this situation causes smart and technologically aware individuals to often successfully escape prosecution or make the trial process long and eroding.

-2Substantive dimensions of criminal protection of classified data

-1 -2Criminalization of criminal behaviors (unauthorized access, eavesdropping, espionage, data forgery and destruction)

Criminalization of cyber criminal behaviors – including unauthorized access, eavesdropping, espionage, data forgery and destruction – is considered one of the most advanced areas of criminal law, which has a strategic position with the growth of information technology and the increase in threats against classified data. (Grayli, 2010, 159-188) Unauthorized access to computer data and systems means intentional and unauthorized entry into systems that are protected by security measures. This behavior, even if it is simply a simple observation of protected data and does not lead to the deletion or modification of information, is considered a crime according to the articles of the Iranian Computer Crimes Law and international standards. The purpose of criminalizing this behavior is to structurally confront intruders, preserve privacy and public order, and prevent security and economic threats, because even non-destructive intrusion can create a platform for more serious crimes such as information theft, espionage, or extortion (Shahmoradi,

2016, p. 2). The criminalization of unauthorized wiretapping and data eavesdropping demonstrates the fundamental importance of the privacy of communications and correspondence in the modern legal order. The Computer Crimes Law in Iran and related articles in comparative legal systems emphasize that any wiretapping, recording, or accessing content and communication data of individuals without the permission of competent authorities and the knowledge or consent of the data owners is an example of serious crimes against fundamental freedoms. In addition to threatening the confidentiality of communications, this crime jeopardizes the integrity of individual freedom and the integrity of data exchange. Ensuring citizen rights, preventing abuse of power institutions, and confronting the development of illegal control mechanisms are important parts of the legal function of criminalizing unauthorized wiretapping (Jazairi et al., 1401, 149, 166).

In the field of computer espionage, criminal treatment of illegal intrusion into national secret and sensitive data plays a vital role in protecting the country's key information; so that in Iran, according to Article 731 of the Islamic Penal Code (Penalties) and related articles in the Computer Crimes Law, any access, disclosure, or provision of confidential data to unauthorized persons, especially if it leads to harm to national security or the country's interests, is prosecuted and severely punished as computer espionage. In addition to providing an efficient legal tool to protect national sovereignty and national data security, this criminalization has a high deterrent coefficient in confronting domestic and foreign espionage networks and reflects the active interaction of Iranian criminal law with current security requirements and global cyber challenges (Rahami and colleagues, 2012, pp. 177-193). From the perspective of data forgery and destruction, Iran's legislative approach is also a necessary response to new challenges related to the authenticity and reliability of digital communications. Data falsification in the form of adding, changing or deleting correct information or producing fake data with the aim of deceiving, illegally exploiting and disrupting the information and economic order of society, such as intentionally destroying or deleting data, causes the collapse of the trust-based order of the digital space. The Iranian Computer Crimes Law (Articles 8-12 and its equivalent in the Islamic Penal Code) has adopted international documents such as the Budapest Convention and has provided for heavy guarantees of execution for these crimes, including imprisonment, fines and even professional deprivations, in order to prevent widespread and irreparable damage and disruption to data and the digital trust system. In the Iranian legal system, the disclosure of classified data and documents is considered a serious example of crimes against national security, and the legislator has severely criminalized this phenomenon in various laws - especially in the Islamic Penal Code and the Computer Crimes Law - with the aim of protecting the national interests and public order of the country. According to Article 505 of the Islamic Penal Code, anyone who “with the aim of undermining the security of the country” collects classified information – whether secret, confidential, top secret or top secret – by any means and intends to make it available to unauthorized persons, shall be sentenced to imprisonment for two to ten years if he succeeds in doing so, and to imprisonment for one to five years if he fails; in this article, regardless of the method of collection or the nationality and position of the perpetrator, the criterion for the commission of the crime is the mere collection of information and the intention to disclose it (Islamic Penal Code, Article 505). Also, in Article 506, the legislator has stipulated that for cases of committing this crime by government officials who are equipped with security training but who, due to negligence and failure to observe protection principles, suffer information leakage, the penalty for imprisonment is one to six months, and the commission of this crime depends on the determination of the inclusion of the description of “enemy” for the recipient of the information (Islamic Penal Code, Article 506).

In committing these crimes, if the context for disclosing data is cyberspace (such as publishing classified information on social networks or websites), Article 731 of the Islamic Penal Code provides for a clear example of "computer espionage," according to which providing secret data in a way that harms the country's security or national interests entails a more severe punishment. Even if the perpetrator is an official or office holder, for the sole purpose of collecting and disseminating classified data or disclosing it through electronic systems, if general and specific malice - that is, knowledge of the classification of the data and the intention to harm national security - is established, the perpetrator will be prosecuted and

punished. There are also special regulations at the level of disclosing military data or specific cases of the armed forces, and the Armed Forces Crimes Law, in Article 24, states that any military that provides classified secrets or documents to the enemy will be considered a war criminal (Armed Forces Crimes Law, Article 24).

Despite the existence of explicit criminalization and a large number of instances, Iranian criminal law still faces challenges in clarifying the instances of classified data and determining the precise boundary between public and confidential data. Also, the legislative practice over the past decade has moved towards reducing classification and supporting the free flow of information, but in the field of national security and sensitive data, a strict approach has been maintained, such that even the intention to disclose and the failure to achieve the result are subject to punishment. Therefore, in order to guarantee fundamental rights and prevent any possible abuse, it is inevitable to review the definition and identification of classified data and improve the transparency of executive procedures so that while maintaining national security, privacy and freedom of access to information are also properly observed.

-2 -2Punishment and its governing principles

Punishment means determining the type, amount and limits of punishment appropriate to each crime in the process of legislation and criminal policy; A process that must not only be based on principles such as justice, proportionality, and purposefulness, but must also be flexible in the face of the requirements of the time, social developments, human rights teachings, and the expectations of society. The principles governing sentencing are a set of fundamental and philosophical criteria that guarantee that punishments are merely a reasonable, proportionate, and effective response to the reform of the victim and public order, and are far from vindictive, authoritarian, and merely symbolic aspects. Accordingly, principles such as justice (proportion between punishment and crime), human dignity (avoiding degrading and inhuman punishments), rationality and effectiveness (targeting punishment for prevention and correction), temporal and spatial proportionality, and compliance with higher-level laws are at the forefront of sentencing policies (Pevandi, 1403, pp. 52-87).

Theoretically, targeted sentencing is an approach that emphasizes the conscious and purposeful selection of a penal response appropriate to the nature of the crime and the offender, the goals set for punishment (prevention, reform, deterrence, and securing the rights of the victim), and considering the sum of the goals between them. The key principles here are the principle of the non-additivity of the goals of punishment (that the goals of prevention, reform, deterrence, and punishment cannot always be added together and fully realized), the principle of the incompatibility of the severity of punishment with the goal (increasing the severity of the penalty does not necessarily lead to a reduction in crime or an improvement in the reform of the offender), and the principle of the necessity of qualitatively assessing legal and social criteria before making a final decision (Haji Dehabadi, 2019, pp. 101-134). In addition to creating a strategy for overcoming stereotypical and emotional punishments, these principles prevent the instrumental and non-targeted use of punishment against vulnerable segments of society. In specialized documents and international authorities, the principles of punishment based on the principles of human rights and the principle of minimalism have also been emphasized. According to Ashworth's view, the criminal law system should resort to punishment only when the perpetrator's behavior has caused serious and real harm to the fundamental rights of individuals or the order of society, and in this case, the principle of proportionality, fairness in the application of justice, and observance of fundamental freedoms must be absolutely observed (Ashworth, 2024, pp. 22-45). The plurality of these principles and their mutual relationship with the cultural, social, and political realities of countries causes the punishment process to have an integrated and dynamic approach, instead of a negative and abstract view, which is also responsive to the continuous changes in society.

-3-2Criminal liability of natural and legal persons

The criminal liability of natural and legal persons has gained additional importance both theoretically and from the perspective of the practical functioning of the judicial system. The criminal liability of natural

persons, based on the principle of individual responsibility, conceptually implies that only human individuals, due to their independent will and consciousness, can be directly addressed for punishment. Traditional rules of criminal law, especially in classical schools, have recognized criminal liability as natural and obvious for natural persons and have considered the realization of the material and spiritual elements of a crime to require the intention, knowledge and will of a human person. For a long time, this traditional approach considered the scope of criminal liability limited to individuals and believed that personality characteristics such as reason, will and consciousness, which are necessary for the attribution of guilt, are realized only in adult and free human beings (Golduzian, 1400, p. 87).

At the same time, with the expansion of the role of legal entities in the social and economic life of societies, new challenges have been raised in the field of attributing criminal liability to institutions such as companies, institutions, associations and other units with legal personality. These developments have led modern legal systems, by adopting different approaches and in contrast to traditional theories, to consider it necessary to accept the criminal liability of legal entities. The theoretical basis of this liability can be seen in the social function of legal entities, the power of extensive influence on public interests and the need to be accountable for organized crime. Modern laws, including Article 143 of the Islamic Penal Code of Iran, also hold legal entities liable in the event of a crime committed by a legal representative and in the name or in line with its interests, and stipulate that this liability does not prevent the liability of the natural person who committed the crime; That is, in committing a crime, both a legal person and a natural person can be held accountable (Mousavi Mojab, 2015, pp. 147-169)

At a comparative level, it should be noted that the scope and limits of criminal liability of legal persons, in addition to the aspect of substantive law, have different practical considerations than natural persons. Imposing penalties such as imprisonment or direct corrective measures, which are possible for individuals, is not possible due to the abstract nature of legal persons, and mainly tools such as fines, liquidation, prohibition of activity and publication of a conviction are used. In advanced legal systems, pluralism is the basis between the approach of "direct liability" (attribution of the crime to the legal entity itself) and "Indirect liability" (attribution to the actions of relevant real actors) is observed. This theoretical and legislative development in Iranian criminal law, adapted from the French and English systems, is also being institutionalized and indicates a legislative and judicial determination to respond to the problems of modern structured and organized crime (Ashworth, 2024, pp. 292-310).

The necessity of accepting the criminal liability of legal entities is not only a temporary response to economic and technological developments, but also a legal necessity to prevent circumvention of the law, criminal exploitation of collective capacities, and protection of public interests. Therefore, any limitation of the aforementioned legal liability can be the source of undue exemptions, the spread of organized corruption, and a decrease in the efficiency of criminal justice. Accordingly, the Iranian legal system, while maintaining the principles of individual responsibility and the need to prove material and moral elements, must continuously reform and update efficient legal instruments for attributing crimes and implementing effective penalties against legal entities in order to ensure deterrence and public rights.

-3Formal dimensions of criminal protection of classified data

-1 -3Crime detection and collection of digital evidence

Crime detection and collection of digital evidence, especially in the field of classified data, is a very complex and specialized process that requires special attention to the technological nature, inherent vulnerability, and legal requirements of this type of information. The first and most important principle in this process is to understand the nature and tools related to the identification, protection and analysis of digital data. The identification steps include determining the data sources (such as computer systems, networks and storage devices) and then securing them to prevent the destruction or manipulation of information; in this regard, it is necessary to observe principles such as making accurate copies, maintaining data integrity through hashing, and recording the chain of custody; because any damage or manipulation can completely destroy the credibility of the evidence in the eyes of the judicial authorities (Casey, 2011, pp. 105-131).

Next, the collection of digital evidence is subject to the scientific and technical principles of digital forensics and requires the storage, retrieval and analysis of information in an accurate and verifiable manner. Digital evidence in this area can include system logs, event log files, electronic messages, user behavioral data and any digitally stored traces. Modern legal systems, including Iran, emphasize the integrity, authenticity, and validity of digital evidence by stipulating it in the Criminal Procedure Code and the Computer Crimes Law. Problems such as ease of change, speed of deletion, and difficulty in validating data are fundamental challenges that make the collection and reliance of digital evidence difficult; however, courts give credibility to this evidence when the process of documenting, protecting, and reconstructing the chain of data transmission and processing has been observed based on international and national standards (Bahrami and Chengaei, 1404, p. 9). The nature of the process of collecting and relying on digital evidence in investigating crimes against classified data is clearly dependent on observing strict formal rules and institutional commitment to legal standards. The possibility of reliance and proving a crime is established when the chain of evidence protection and ensuring the integrity and inviolability of data are continuously observed; The slightest disruption in this cycle, whether due to documentation deficiencies or negligence in storage, can bring the entire criminal prosecution process to a standstill and even lead to the rejection of all evidence by the judicial authority. In this context, the legal function of digital evidence is not limited to collection and presentation, but rather the assessment of its validity and authenticity and its direct connection to the legitimacy of the judicial decision becomes an inevitable link.

-2-3Jurisdiction and related challenges

The extraterritorial and borderless cyberspace is of such a nature that it severely challenges the traditional principles of territorial jurisdiction; in such a way that the simultaneous occurrence of the elements of a crime (including criminal conduct, harmful consequences, and means of committing a crime) in several different countries makes it very difficult to determine the competent authority for the investigation. In this regard, various theories have been proposed for determining jurisdiction: implementing traditional rules with a new perspective (such as the place of occurrence of the result or behavior), accepting cyberspace as an international free space, establishing a special cyber court, or granting jurisdiction to a court that is logically related to the crime; for example, Iran's criminal regulations have moved towards a combination of these models by amending Article 28 of the Computer Crimes Law, but serious shortcomings still remain (Heidari and colleagues, 1401, pp. 1-22). At the international level, the challenges of jurisdiction in cybercrimes are mainly due to the territorial interference of legal systems and the lack of a single procedure in relations between states. Principles such as "territoriality", "personality", "protection of national interests", and the principle of "universal jurisdiction" have each provided incomplete answers to this dilemma; but geographical borders and national sovereignty often prevent effective cooperation to pursue and punish cybercriminals. Issues such as inconsistent regulations, lack of acceptance of the principle of double criminality, difficulty in obtaining and adducing international evidence, and complexities related to judicial representation effectively leave many cybercriminals open to escape. More importantly, the emergence of conflicting or overlapping jurisdictions may hinder prosecution and undermine criminal justice (Goldsmith, 1998, p. 1205).

The widespread overlap of legal jurisdictions, the lack of overlapping frameworks for dispute resolution, and the complexity of the rules of representation or extradition have become a fundamental problem for the administration of justice. The incomplete functioning of traditional principles such as territoriality or personality has, in practice, caused digital criminals to exploit the multiplicity of involved territories and the difference in criminal standards to circumvent criminal liability or find legal shelter. This situation upsets the balance between national judicial authority and the need for cross-border cooperation, and turns the implementation of criminal justice in the realm of cyber data into a harmful and sometimes fruitless postponement.

-3 -3The role of the FATA Police and other relevant institutions

The FATA Police, as the specialized arm of the Islamic Republic of Iran’s law enforcement force in combating cybercrime, is responsible for the mission of crime detection, identification, prosecution, and

collection of digital evidence by equipping its forces with up-to-date knowledge in the field of information technology and employing technological systems. On the one hand, this institution plays its role in preventing crimes by conducting virtual patrols, monitoring data networks, using smart analysis technology, and setting up warning systems for users and institutions. On the other hand, it cooperates with the judicial system to collect evidence, monitor criminal behavior, and deal with those who disclose, steal, or destroy classified data. Specialized training and improving the knowledge of the FATA police, increasing the number of experienced human resources, and cooperating with other security and intelligence agencies are essential requirements for successfully fulfilling this role (Masoudian, 2012, p. 107). In addition to the FATA police, other related institutions such as the Ministry of Intelligence, the Passive Defense Organization, national data centers, and the judicial system are also active in the field of protecting classified data and criminally prosecuting violations against this data. These institutions play a decisive role in policymaking, developing protective regulations, determining information security standards, and assessing risk. Interdepartmental cooperation between the FATA Police and other organizations, especially in the areas of information exchange, identification of criminal chains, and tracking of leaked or destroyed data in the international space, is a vital necessity, the realization of which requires the development of common procedures, technical training, and complete information coordination. Also, specialized committees in the Supreme Council for Cyberspace and judicial institutions have found a special place in the field of handling sensitive data crimes, and joint guidelines have been developed for a coordinated confrontation with emerging threats, technology, and challenges (Akbarzadeh et al., 2022, p. 15 PDF).

The operational focus of the FATA Police on the use of new technologies, data-based analysis, and human resource empowerment plays a pivotal role in the effectiveness of the process of detecting and pursuing cybercrime. The organized interaction of the FATA Police with an institution such as the Ministry of Intelligence or the Passive Defense, with the aim of joint policy-making and exchange of operational data, creates a legal and executive barrier against systemic disruptions and abuse of institutional gaps. In this description, the combination of operational expertise, protective regulation and interdepartmental coordination has led to a comprehensive strategy in confronting criminal behavior against sensitive data, such that any inefficiency in one of these aspects can disrupt the criminal protection chain and allow for widespread damage to the privacy of classified data.

-4 -3International cooperation in the prosecution of cybercrimes

Cyberspace, with its open, vast and cross-border nature, allows criminals to take advantage of geographical restrictions to evade judicial prosecution, hide identities, quickly transfer illegal data and carry out organized crimes; Therefore, only bilateral or national cooperation is not efficient, and international institutions, the creation of multilateral treaties, and the development of joint enforcement mechanisms are considered the main foundation of global criminal policy (Shahbazi, 2017, 7). One of the most important achievements in this field is the ratification of the Budapest Convention in 2001, which, as the first and most comprehensive international document in the fight against cybercrime, facilitates cooperation between countries in the field of determining instances of crimes, collecting electronic evidence, extradition of criminals, and exchanging information. This convention not only proposes uniform definitions and coordinated frameworks for cybercrime, but also develops in Chapter Three the principles of effective cooperation between states, the designation of 24/7 contact points, and the design of rapid methods for judicial representation and data transfer. Accession to this Convention or the establishment of similar mechanisms will lead to the harmonization of laws, reduce conflicts of jurisdiction, and expedite the prosecution of crimes in the digital space, and is particularly important in combating the disclosure of classified data and protecting victims (Gercke, 2012, p. 26; Council of Europe, 2001).

A critical review of the state of international cooperation in the prosecution of cybercrimes shows that the adoption of the Budapest Convention and similar global experiences have played a fundamental role in the development of procedural convergence, rapid exchange of information, and extradition of criminals. The legal frameworks of these treaties, by providing clear rules for the sharing of evidence, coordination of

jurisdictions, and technical requirements for the transfer of digital data, provide structural solutions to overcome the barriers of national jurisdiction and traditional gaps in criminal law in cyberspace. This cooperation model led to the harmonization of domestic laws, reduced conflicts of jurisdiction, and increased the efficiency of criminal prosecution in the field of classified data, and was able to enhance the ability of national agencies to combat cross-border crimes in an unprecedented manner. 4- The need to review and amend laws

-1 -4Existing legislative and executive challenges in Iran

Legislative and executive challenges of criminal protection of classified data in Iran mainly relate to the inefficiency, fragmentation, and inadequacy of existing laws. Current laws such as the Computer Crimes Law (approved in 2009) and related guidelines, although they have created an initial framework for protecting sensitive data, lack conceptual comprehensiveness, precise determination of instances of classified data, and systematization of protective measures commensurate with the level of threat. These shortcomings have caused confusion in the judicial process and executive institutions in interpreting, implementing, and enforcing regulations, and as a result, the effectiveness of criminal protection has been greatly reduced; In addition, in many cases, the line between the misuse of ordinary data and data of national or economic importance is not clearly defined.

In terms of implementation, serious challenges are seen in the interaction between relevant institutions, the weakness of technical infrastructure and the lack of unified protocols for collecting, protecting and citing digital evidence. The lack of sufficient specialized training for officers and judges, the lack of widespread use of new data identification and analysis technologies, and operational incoherence between the police, prosecutors and technical experts, cause the process of pursuing crimes against classified data to often remain fruitless or become time-consuming and eroding. Also, establishing and maintaining the chain of authenticity and integrity of data has become a difficult task; because the ambiguity in the manner of storing and transferring data weakens judicial security and the deterrent function of the criminal justice system. (Moazinzadegan et al., 1401, 37-73)

The lack of coherence in the legislative approach in clearly determining the instances, scope, and supporting processes has caused the principle of legality of crimes and punishments to fail to provide an appropriate response to rapid technological developments and the emergence of new instances of vital data. This situation has caused confusion in legislative policymaking, judicial procedures, and the performance of executive institutions; in such a way that not only is it rarely possible to effectively prosecute data criminals, but also doubts about the nature of data, its hierarchy of importance, and appropriate protective measures often weaken deterrence and even undermine public trust in criminal justice in the digital arena. This fragmentation and weak enforcement indicate that the current challenge is not simply due to a legal deficiency, but rather to the lack of a grand strategy, institutional risk assessment, and weak interaction between the main players in criminal policy.

-2-4Comparison with international experiences and standards

The criminal protection system for classified data in Iran faces a significant conceptual, executive and institutional gap compared to international standards and experiences, especially the EU General Data Protection Regulation model. In the EU legal system, personal data is broadly and comprehensively defined, and a clear hierarchy has been established for sensitive data, data processors and data controllers, data subject rights and institutional control and oversight mechanisms. The fundamental theoretical and practical principle of this system emphasizes the principle of informed consent of data owners and transparency: any processing of personal data requires written and informed consent, clear purpose determination and the possibility of exercising the “right to be forgotten”. In this framework, the commitment to immediate notification of data breaches, the secure cross-border flow of information only with countries that have a similar level of protection, the designation of an independent supervisory authority in each member state, and the imposition of effective and progressive fines (up to €20 million or 4% of companies’ revenue) have effectively provided a strong guarantee for the realization of criminal and

civil protection of classified data (Custers et al., 2018, p. 236; Bart Custers et al., Computer Law & Security Review, 34(2)).

In Iran, despite the adoption of the Computer Crimes Law of 2009 and efforts to develop a comprehensive plan for the protection of personal data, the gap of a comprehensive, coherent, and accountable system is still evident. The personal data protection plan proposed by the Parliament, inspired by the GDPR and some US and French laws, has attempted to provide a similar structure; However, the negative approach, ambiguity in the definition of data ownership, the lack of a clear system of consent and notification to users, the lack of an independent supervisory body, and the lack of effective enforcement guarantees have limited the protective nature of this plan. In practice, the lack of distinction between ordinary and classified data, the lack of transparency of the processor's responsibilities, and the disregard for new principles such as "privacy by design", "processing impact assessment" and "data breach notification" have caused the implementation of criminal protection to face serious challenges and is mainly limited to penalties based on references to the Islamic Penal Code, which lacks deterrent effectiveness compared to the progressive penalties of the GDPR. The criminal protection system for classified data in Iran compared to international models such as the GDPR clearly shows that the current gap is not a purely legislative challenge, but rather a result of the lack of institutionalization of concepts such as data transparency, data subject rights, and an independent oversight mechanism. In the European legal framework, the mechanism of continuous cooperation between the user, the controller and the supervisory authorities has been able to create an operational model for the real enforcement of individuals' rights and active accountability, while the Iranian system is still based on ex post control, symbolic penalties and a lack of institutional accountability. This structural difference seriously undermines the effectiveness of the domestic protection system in responding to new data risks and pursuing serious breaches, as it not only lacks sufficient deterrent tools, but also leaves the risk of data breaches redistributed at the level of data owners, and as a result, criminal protection in practice loses its desired function and fundamental support.

Conclusion

The conclusion of this research in the field of criminal protection of classified data in the computer space shows that although the Iranian legal system has taken important steps in the field of criminalization of some threats, there are still serious weaknesses in various dimensions. Classified data is considered as the lifeblood of national security and a strategic asset in the economic and social fields, and its protection is an inevitable necessity. The studies revealed that Iranian regulations, especially the Computer Crimes Law, cover some important instances such as unauthorized access, eavesdropping, forgery, and destruction of data, but the lack of legislative coherence and comprehensiveness in these laws is an obstacle to the realization of complete criminal protection. The findings show that the biggest challenge in criminal protection is the inadequacy of formal mechanisms such as crime detection, collection of digital evidence, and determination of jurisdiction. Although the FATA Police and other relevant institutions have played a role in this regard, the weakness in specialized training, lack of technical facilities, and lack of precise regulations have reduced the efficiency of these processes. On the other hand, the characteristics of cyberspace, such as its transnational nature, make international cooperation doubly important, while Iran has not yet joined key conventions such as the Budapest Convention, which poses serious limitations for the prosecution of cybercriminals. In the substantive dimension, criminal protection also faces problems. One of the most important of these is the lack of comprehensive criminalization for some more complex cyber behaviors, such as computer espionage at strategic levels or attacks on critical infrastructure. Also, the punishment in existing laws is sometimes not proportionate to the level of threat or damage to classified data, and this can lead to the ineffectiveness of punishments. In addition, the criminal liability of legal entities in this area requires further review and clarification, because a large part of sensitive data is in the possession of organizations and institutions. From another perspective, a comparative comparison with advanced legal systems showed that many countries, relying on international regulations and utilizing modern technologies, have adopted more effective methods in dealing with threats against classified data. A clear example of this is multilateral cooperation and immediate exchange of information between countries to identify and prosecute cyber attackers. These experiences can be valuable guidance for the

Iranian legal system, especially in conditions where Internet threats are spreading without borders and at high speed. Therefore, the answer to the main research question is clear: Although the Iranian criminal law system has been able to provide some criminal protection for classified data through substantive and formal regulations, it has not been able to provide complete and efficient protection. The research hypothesis of the existence of legislative gaps and implementation challenges was also proven, showing that lack of coherence, weakness in crime detection mechanisms, and lack of international cooperation are among the most important obstacles. Therefore, it can be concluded that reviewing domestic laws, strengthening the training and capacity of responsible institutions, more accurately criminalizing emerging behaviors, increasing the proportionality of penalties, and joining international documents can be practical and effective steps to ensure the security of classified data in Iran's computer space. The realization of this will not only lead to the promotion of public trust and the security of the digital space, but will also lead to the preservation of national integrity and authority in the political and economic arenas.

- To enhance criminal protection of classified data in the computer space, the first practical solution is to review and amend existing laws. In this context, a more comprehensive criminalization of new cyber threats such as computer espionage, attacks on critical infrastructure, and intentional violations of the integrity of sensitive data should be carried out. The proportionality of penalties to the level of threat and damage incurred should also be reviewed in order to create real deterrence. In addition, it is necessary to clearly and effectively foresee the criminal liability of legal entities, because many confidential data are in the possession of government and private organizations and in the event of negligence or abuse, they must be held accountable. Another solution is to strengthen the responsible institutions and enforcement mechanisms. The FATA police and the judiciary should receive specialized training and advanced equipment to detect cyber crimes and collect digital evidence. Developing international cooperation through accession to authoritative documents such as the Budapest Convention and establishing mechanisms for exchanging information between countries will enable the effective prosecution of transnational criminals. In addition, culture building and training at the level of organizations and even among users can prevent security breaches caused by human errors or carelessness and complete the cycle of protecting classified data.

References

- Bahrami, Alireza; Chengaei, Sajjad (1404). “Investigation of types of electronic evidence in proving computer crimes”, Fifth International Conference on Advocacy, Law and Humanities.
- • Peyvandi, Gholamreza (1403). Sentencing: Foundations, Principles, Criteria and Challenges. Islamic Culture and Thought Research Institute Publication Organization.
- • Jazayeri, Seyed Abbas; Mahmoud Shahrani (2016). “Listening to Conversations from the Perspective of Iranian Criminal Law, Imamiyyah Jurisprudence, International Documents and Conventions”, Jurisprudence and Modern Law, Volume 3, Issue 9, pp. 149-166.
- • Khorsandi, Hamid Reza; Sobhaninia, Zahra (1402). “Analysis of the Criminalization of Data Forgery and Destruction in the Iranian Computer Crimes Law”, Information Technology Law, Year 5, Issue 3, p. 242.
- • Rahami, Mohsen; Sirous Parvizi (1391). “Computer Espionage in Iranian Law and Its International Status”, Private Law Studies, Volume 24, Issue 3, pp. 177-193.
- • Shahimoradi, Khairollah (1395). “Legal Study of the Crime of Unauthorized Access to Data and Computer Systems in Iranian Law”, First National Conference on Futures Studies, Humanities and Social Security.
- • Kazemi, Mohammad Reza (1401). “Computer Espionage in Iranian Law and Compliance with International Documents”, Modern Criminal Law Research, No. 12, p. 128.
- • Golduzian, Iraj (1400). General Criminal Law, Volume 1. Tehran: Mizan Publishing.

- • Computer Crimes Law of the Islamic Republic of Iran, approved in 1388.
- • Islamic Penal Code, approved in 1392 and subsequent amendments.
- • Penal Code for Publishing and Disclosing Confidential and Secret Government Documents, approved in 1353 and subsequent amendments.
- • Executive Regulations on the Method of Identifying and Classifying Secret Data, approved by the Supreme National Security Council and the Ministry of Intelligence.
- • Masoudian, Mohsen (1391). "The Role of the Police in Preventing Cybercrimes and Ensuring Security in Cyberspace (FATA Police)", Social Order, Year 1, No. 1, pp. 103-125.
- • Moezinzadegan, Hassanali; Amiri, Saeed (1401). "Legislative and Judicial Challenges of Scientific Evidence in Iranian Criminal Law", Researches in Criminal Law and Criminology, Volume 10, Issue 19, pp. 37-73.
- • Yabloei, Hossein (2017). "Challenges of Iranian Criminal Law Regarding the Protection of Privacy in Cyberspace", Master's Thesis, Faculty of Law, University of Tehran.
- English Sources
- Aldurra, Ahmed (2013). Cybercrime and Penal Code: A Comparative Study. Dubai Police Academy, p. 63.
- Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd Edition. Syngress, pp. 50-54.
- Ashworth, Andrew (2024). Principles of Criminal Law. Clarendon Law Series, pp. 22-45.
- Ashworth, Andrew (2024). Principles of Criminal Law. Ninth Edition, Oxford University Press, pp. 292-310.
- Bakare, O. et al. (2024). "A Systematic Analysis of Data Protection Regulations," Proceedings of the 58th Hawaii International Conference on System Sciences, p. 4450.
- Bart Custers, Francien Dechesne, Alan M. Sears, Tommaso Tani, Simone van der Hof (2018). "A comparison of data protection legislation and policies across the EU." Computer Law & Security Review, 34(2), pp. 234-243.
- Bertino, E., & Sandhu, R. (2005). "Database Security – Concepts, Approaches, and Challenges." IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19.
- Casey, Eoghan (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd Edition, Academic Press, pp. 105-131.
- Casey, Eoghan (2019). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th Edition, Academic Press, p. 411.
- Council of Europe. (2001). Convention on Cybercrime, Budapest.
- Custers, Bart; Dechesne, Francien; Sears, Alan M.; Tani, Tommaso; van der Hof, Simone. (2018). "A comparison of data protection legislation and policies across the EU." Computer Law & Security Review, 34(2), pp. 234-243.
- Dashti, B. (2019). "Comparative study of cyber-crime in Iran and international law." Journal of Law and Political Sciences, University of Mazandaran, 11(1), 1-18.
- Frantz, P., & Nowklass, S. (2017). "Information Classification and Data Protection." Information Systems Management Journal, 34(1), 47-59.
- Fung, B., & Chowhan, S. (2020). Data Classification: Theory and Practice. Springer, p. 112.
- Gercke, Marco (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU, p. 26.

- Goldsmith, Jack L. (1998). “Against Cyberanarchy,” University of Chicago Law Review, vol. 65, no. 4, pp. 1199-1226.
- Peltier, T.R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications, pp. 31-36.
- Pazhohan, H. (2023). Global Data Protection Standards: A Comparative Analysis of GDPR and Other International Privacy Laws. Legal Studies in Digital Age, 2(3), p. 4.
- Whitman, M.E. & Mattord, H.J. (2017). Principles of Information Security. 6th Edition. Cengage Learning, pp. 19-24