How to cite this article:
Khaneyousefi, K., & Mohammadnejad, P. (2026). An Examination of Recidivism and Concurrence of Crimes in Iran's Criminal Law in Comparison with Turkey and Their Consequences for Cybercrimes. *Journal of Historical Research, Law and Policy, 4*(2), 1-12. https://doi.org/10.61838/jhrlp.164

Article history:
Original Research

Dates:
Submission Date: 17 September 2025
Revision Date: 14 December 2025
Acceptance Date: 21 December 2025
Publication Date: 01 March 2026

An Examination of Recidivism and Concurrence of Crimes in Iran's Criminal Law in Comparison with Turkey and Their Consequences for Cybercrimes

1. Koroush. Khaneyousefi [1] : Department of Law, ST.C., Islamic Azad University, Tehran, Iran
2. Parviz. Mohammadnejad [2*]: Department of Law, ST.C., Islamic Azad University, Tehran, Iran

*corresponding author's email: P_mohammadnejad@azad.ac.ir

ABSTRACT

Any change or transformation in the contemporary world inevitably entails certain effects and consequences, such that with the invention of any new instrument there is always the possibility of its misuse. In this regard, the science of law encompasses anything that may cause even the slightest disruption to this balance and seeks to eliminate or prevent its undesirable effects. Cyberspace is no exception to this rule and has exerted both positive and negative impacts on human life, rendering the necessity of studying it undeniable. Consequently, criminal policymakers, legal scholars, and criminologists have entered this domain and, by defining cybercrimes, prescribing proportionate punishments, and proposing and implementing security and preventive measures against the risks of this environment, as well as educating and raising public awareness about the harmful consequences of cyberspace, have fulfilled their fundamental responsibilities in this field. Examining the quality and dimensions of these functions is therefore essential. In this article, the nature of cyberspace and communication tools, along with their definition, historical background, characteristics, and classification, are examined in the contexts of Iran and Turkey. The potential risks and the globalization of efforts to combat cybercrime are presented as key conclusions of the discussion. Moreover, certain proposals are offered as a model for criminal policymakers in Iran and Turkey to confront and prevent cybercrimes, which it is hoped will attract the attention of legal scholars, criminologists, and users.

Keywords: *Cybercrimes; International Law; Law of Iran and Turkey.*

Introduction

Undoubtedly, every activity requires appropriate tools, and the instrument for realizing a modern society is information and communication technology. The original purpose of inventing the computer was to accelerate and facilitate information processing, a goal that was successfully achieved, while telecommunications, as the most important communication tool, have played a significant role in disseminating this processed information. Over approximately the past half century, with the gradual discovery of the remarkable capabilities arising from the integration of these two technologies, a revolution occurred in the field of information and communication technology. The peak of this revolution can be observed in the emergence of global computer-based information networks which, since the 1990s, have brought about a fundamental transformation in this domain. These networks, themselves composed of numerous interconnected computer systems, communicate through advanced

telecommunication technologies and have created a space with characteristics entirely distinct from the physical world. Some have termed this space “virtual space,” while others have chosen the designation “cyberspace.” In addition to providing opportunities for human growth and development, cyberspace has also created opportunities for criminals. Consequently, contemporary discourse refers to the “dark side” of the Internet. Among the characteristics of this environment is that offenders can commit crimes more easily, perpetrate a greater number of offenses, and target a wider range of criminal objectives. These features of cyberspace have led to the enactment of regulations concerning criminal responses to offenders in Iranian law, international law, and the law of Turkey. This article seeks to answer the following questions.

Research Questions

How are cybercrimes in Iran and Turkey aligned from a legal perspective?

What is the deterrent power of current punishments with respect to computer crimes?

In which domains can cybercrimes be committed?

This article is written based on a descriptive–analytical method. After examining and analyzing the Computer Crimes Law of Iran and the relevant legal framework of Turkey, it describes and analyzes cybercrimes. It should be noted that the present research has been conducted using documentary and library-based methods.

Cybercrimes in Iran: Recidivism and Concurrence

Legal Framework:

The Islamic Penal Code and its relevant provisions across different periods, as well as certain specific laws such as the Computer Crimes Law enacted in 2009 and its subsequent amendments, constitute the primary legal framework governing cybercrimes in Iran.

Criminal Justice Enforcement Mechanisms:

These include public prosecutors’ offices, general and specialized courts, and supplementary punishments such as prohibitions on engaging in similar activities or judicial supervision.

Recidivism in Iran:

In Iranian criminal jurisprudence, the concept of recidivism is generally addressed through terms such as “prior convicted offender” or “repetition of crime.” In certain statutory provisions, perpetrators of specific crimes, including computer-related offenses, face aggravated punishments following a prior conviction. For example, in some economic or cybercrimes, a prior criminal record may result in increased penalties or the imposition of supervisory conditions. Although there is not always a single codified provision dedicated exclusively to recidivism, the general principles of sentence aggravation for repeated offenses are applied. In judicial practice, prior records are considered as aggravating factors, provided that the prior conviction is established and is relevant to the current offense (1).

Concurrence (Multiple Offenses) in Iran:

In certain cybercrimes, each unlawful act is regarded as an independent offense, such as unauthorized access to multiple systems. In other cases, the legislator may treat offenses either as separate crimes or as multiple

offenses within a single پرونده. Judgments may impose combined or consecutive punishments due to the commission of multiple offenses. Courts may also consider administrative sanctions, including dismissal from employment or prohibition from technology-related activities.

Practical Note:

In cybercrime cases, factors such as prior criminal records, level of access, extent of damage, severity of losses, the role of employees or insider attackers, and the existence of compound crimes (for example, unauthorized access combined with fraud) are influential in aggravating or mitigating punishment (2).

Cybercrimes in Turkey: Recidivism and Concurrence

Legal Framework:

Turkey's criminal and civil liability regime, particularly the Turkish Penal Code, which has undergone updates in recent years, forms the basis of cybercrime regulation. Cybercrimes in Turkey are defined under categories such as unauthorized access, system intrusion, dissemination of confidential information, electronic fraud, and offenses related to information technology services. In addition, specific laws or subsidiary regulations concerning cybersecurity and data protection are in force (3).

Recidivism in Turkey:

The concept of recidivism is explicitly addressed in Turkish criminal law and generally leads to aggravated punishment, particularly when a subsequent offense is committed after a prior conviction. In certain provisions, the frequency of repeated offenses or engagement in cybercrime is incorporated into the determination of penalties. Moreover, for crimes involving significant damage or attacks on critical infrastructure, a prior criminal record may play a decisive role in determining the severity of punishment (1).

Concurrence (Multiple Offenses) in Turkey:

The combination of multiple cyber offenses may result in consecutive or cumulative sentences. In some cases, courts may treat multiple offenses as a single aggravated crime or as several independent crimes. Turkey's legal policy in the field of cybercrime, in light of increasing threats, tends toward harsher penalties where multiple cyber offenses have occurred.

Practical Note:

In Turkey, the role of data and economic damage, the nature of cyber networks, and connections to organized crime can influence judicial decisions regarding recidivism and concurrence. Coordination with data protection and privacy legislation is also significant in cybercrime cases (1).

Comparative Analysis with a Focus on Cybercrimes

Similarities:

Both countries recognize the concept of recidivism as a basis for aggravating punishment in cases involving prior criminal records.

In both systems, cybercrimes are assessed with reference to the rate of damage, the severity of harm to systems and data, the offender's internal or external access, and the level of authorization.

Certain cybercrimes are treated as independent offenses in both jurisdictions, with the possibility of aggregating multiple offenses within a single case or across successive cases.

Differences:

Legislative Trajectory: Iran emphasizes domestic legislation with frequent amendments to cyber laws and penalties, whereas Turkey operates within a more modern criminal framework with more extensive legislative updates aimed at cybersecurity.

Aggravation Approach: Turkey may place greater emphasis on aggravating punishments for repeat cyber offenses, particularly in light of economic losses and threats to infrastructure. Iran adopts a similar approach, but its application may differ due to judicial structure and procedural practices.

Aggregation of Offenses: The methods for calculating recidivism and concurrence differ, potentially leading to variations in sentence aggravation or the imposition of additional sanctions such as activity bans, enhanced fines, or prolonged supervision.

Practical Implications for Research and Legal Practice

Careful examination of the precise statutory provisions governing cybercrimes in each country, with attention to the most recent legislative amendments.

Consideration of criminal records and the manner in which they are recorded and utilized in subsequent prosecutions as aggravating factors.

Distinguishing between multiple cyber offenses within a single case and their simultaneity or continuity in sentencing calculations.

Analysis of economic losses and impacts on critical infrastructure as reinforcing factors for sentence aggravation or the imposition of post-release restrictions.

Review of comparative sources and international standards on recidivism and concurrence in cybercrime and their adaptation within domestic legal systems (4).

Research Findings

Definition of Cybercrime

The first difficulty in providing a definition lies in the very nature of cybercrime. With respect to the definition and nature of crimes, no single uniform model has been followed. In order to understand the concept of cybercrime and to distinguish it from other computer-related crimes, it is necessary to first understand the definition of the cyber environment and its characteristics. Lexically, the term "cyber" in various dictionaries conveys meanings such as virtual and intangible. Despite the absence of a precise dictionary definition of cybercrime, legislators and law enforcement authorities worldwide have come to recognize cybercrime when they encounter it. The dissemination of computer viruses and worms, the execution of electronic attacks, and, in general, any activity that causes disruption to computer networks and the processes based on them are referred to as cybercrimes. In a broad sense, cybercrime can be defined as any activity that exploits computer networks for the purpose of committing criminal acts. Based on this definition, actions such as electronic attacks against critical and national infrastructures, fraud,

electronic money laundering, criminal misuse of the Internet, identity forgery, and even the use of computers and information technology concepts in the commission of non-cyber crimes constitute instances of cybercrime. Overall, it can be stated that cybercrime is a subset of computer crime (2, 3).

Characteristics of Computer Crimes

Classical Crimes with a Cyber Description

This category includes offenses that are traditionally regarded as conventional crimes but, due to technological advancement, are now committed through cyber means. Cybercrimes can generally be classified into four broad categories. Examples include cyber fraud, cyber forgery, cyber sabotage, cyber espionage, and similar offenses (1).

Crimes against the Confidentiality of Data and Systems

Any symbol of subjects, concepts, or instructions—including text, sound, or image—used for communication between computer systems or for processing by a person or a computer system, and generated by a computer system, is considered data content. Crimes in this category include the unauthorized interception of telecommunications data in private communications or classified data that possess value for the internal and external security of a country (4).

Crimes against the Integrity and Availability of Data and Systems

Acts such as alteration, creation, deletion, or disruption of computer and telecommunications systems with the intent to commit fraud, render data unusable, destroy or interfere with data or electromagnetic signals, or prevent authorized persons from accessing data through changes in access codes or encryption are among the crimes included in this category (5).

Content-Related Crimes

This category encompasses crimes in which the computer is used by the offender as a tool or instrument for committing the offense, and information technology merely provides the context for their commission. For example, the dissemination of obscene content—such as the display of male or female sexual organs or sexual intercourse—promotion, incitement, or encouragement of sexual deviations or suicide through computer or telecommunications systems fall within this category (6).

Possible Strategies for Combating and Preventing Computer Crimes

It is the responsibility of the governing system to provide the necessary legal and executive instruments for combating and preventing crimes in light of global developments. The experience of countries with at least a decade of legislative and institutional activity in the field of cybercrime demonstrates that they have sought to establish a balance between societal needs and adequate enforcement guarantees for law enforcement authorities. Not only the three principal institutions—namely the legislature, the judiciary, and the police—but also numerous organizations and ministries have cooperated to implement crime-control strategies through public education and the prosecution of offenders (7).

Principles of Criminal Jurisdiction Concerning International Offenders

Cybercrimes transcend geographical borders, and as a result, the location of the offense and the country suffering harm may differ. For example, if an individual of Turkish nationality disseminates a virus in Turkey and that virus causes damage to a company in the United States, the question arises as to which country's law should apply in punishing the offender. The principles of criminal jurisdiction applicable to international crimes are generally divided into territoriality, active personality, passive personality, protective jurisdiction, and universality. Based on the above example, each of these principles can be explained as follows.

Territorial Principle

This principle refers to the application of national law to all crimes committed within the territory of a state, regardless of the offender's nationality. According to this principle, when an individual commits a crime in Turkey, Turkish law should be applied. However, under the principle of ubiquity, if the crime has also produced effects in the United States, jurisdiction may fall within the competence of that country. If Turkey has no law criminalizing the act, the conduct would not be considered a crime under Turkish law, and consequently the jurisdiction would not be limited solely to Turkey.

Active Personality Principle

The active personality principle entails the application of the offender's national law irrespective of the place where the crime was committed. Under this principle, even if the offense was committed in the United States, but the offender is a Turkish national, only Turkey would have jurisdiction. If Turkey lacks a law addressing the offense, the act would not be criminalized and the principle of legality would prevail.

Passive Personality Principle

This principle holds that the courts of the victim's country have jurisdiction over the offense. According to this approach, the victim's country—in this example, the United States—would have jurisdiction rather than Turkey. However, this principle has not been widely adopted at the international level and no binding treaty has been concluded on its basis.

Protective Principle

The protective system means that regardless of the country in which the offense was committed or the nationality of the offender and victim, the law of the state whose fundamental interests have been harmed is applicable. Under this principle, if a company in the United States is harmed by the criminal act, the matter falls within U.S. federal jurisdiction. Nevertheless, offenses relating to national interests may fall under the laws of both countries, with federal jurisdiction exercising discretion in providing protection.

Universality Principle

Universality refers to the exercise of jurisdiction by any state over certain specific crimes—such as piracy or war crimes—regardless of the place of commission or the nationality of the offender or victim. In this context, crimes

recognized under universal jurisdiction include piracy, war crimes, and crimes against humanity, as determined by international bodies. Accordingly, under this principle, the United States would not have exclusive jurisdictional mechanisms for prosecuting such crimes.

Resolutions of the International Telecommunication Union

The International Telecommunication Union has issued several resolutions related to cybercrime, although they do not directly address the issue through explicit criminal regulations. Among the most important resolutions is Resolution No. 130, adopted at the ITU Plenipotentiary Conference held in Guadalajara, Mexico, in 2010, concerning the strengthening of the role of the ITU in building confidence and security in the use of information and communication technologies. This resolution emphasized the Union's responsibility to cooperate with member states, particularly developing countries, in adopting appropriate and implementable measures to protect against cyber threats, including capacity-building activities in developing national strategies, legislation and their enforcement, and organizational structures such as warning, monitoring, and response mechanisms (1).

Resolution No. 149, adopted at the ITU Plenipotentiary Conference held in Antalya, Turkey, in 2006, addresses the study and examination of definitions and terminology related to building confidence and security in the use of information and communication technologies (8).

Resolution No. 50, adopted at the World Telecommunication Standardization Assembly in Johannesburg, South Africa, in 2008, focuses on cybersecurity (9).

The Legislative Development of Iran's Computer Crimes Law

Given the rapid advancement of computers and their numerous and diverse applications across different sectors, the possibility of misuse of this industry, and the inadequacy of ordinary criminal laws in responding to issues of computer crime, during the process of revising part of the Islamic Penal Code (Taʿzīrāt), the Council of Ministers resolved that the necessary examinations should also be conducted regarding computer crimes and, where specific proposals existed, they should be incorporated into the text of the new Taʿzīrāt bill. Two draft texts were proposed: one by the Secretariat of the Supreme Council of Informatics and the other by the Central Bank. These proposals were reviewed in the Government Bills Commission, and ultimately a bill entitled "How to Deal with Computer Crimes" was approved in the Council of Ministers session dated 27 August 1994, pursuant to which a chapter consisting of two articles was to be added to the Islamic Penal Code. Unfortunately, this bill was not approved by the Islamic Consultative Assembly. Despite the efforts of experts and legal scholars, no chapter or statute under this title was added to the Islamic Penal Code.

From approximately the late 1990s and the early 2000s, various measures were adopted at different levels of governance concerning the necessity of confronting criminal cyber misuse. Among the most significant was a directive issued in 2001 regarding computer-based information networks, which may be regarded as a charter of national criminal policy on computer crimes. In addition to its criminal-law dimensions, this policy document contains valuable preventive measures, and attention to and adherence to it can substantially address problems in this field.

Beginning in 2002, renewed activity in the area of computer crimes commenced, resulting in the preparation of a draft on computer crimes within the Judiciary's Supreme Council for Judicial Development. Ultimately, after a period of 15 years (from the time of its earlier approval within the Council of Ministers), the Computer Crimes Bill was prepared and proposed by the Supreme Council for Judicial Development, and in June 2009 it was approved

by the Islamic Consultative Assembly and confirmed by the Guardian Council. This law (the Computer Crimes Law) consists of three parts and fifty-four articles. Part One addresses crimes and the punishments prescribed by the statute, classifying offenses across seven chapters and addressing aggravated sentencing in an eighth chapter (2).

Chapter One, entitled “Crimes against the Confidentiality of Data and Computer and Telecommunications Systems,” recognizes unauthorized access, unauthorized interception, and computer espionage as instances of this category. The maximum penalties for such crimes when committed by ordinary individuals are set at a fine ranging from 20 million to 60 million rials and imprisonment from one to three years. The actus reus of these offenses resembles crimes against security in the physical world, with the principal difference being the change in the instrumentality of the crime (10).

In Chapters Two and Three, the legislator addresses “Crimes against the Integrity and Availability of Data and Telecommunications Systems,” the actus reus of which may be likened to crimes against property and ownership. In these chapters, offenses such as computer forgery, destruction and disruption of computer systems, and computer-related theft and fraud are addressed. The maximum penalty for computer forgery is prescribed as imprisonment from one to five years and a fine ranging from 20 million to 100 million rials. It appears that, given that computer-related theft and fraud often begin with the forging of a well-known website, the legislator has provided a comparatively severe punishment for this offense relative to other crimes in this section (4).

Chapter Four addresses crimes against chastity and public morality and sets out the instances of obscene content. The actus reus of these offenses corresponds to crimes against public morality, as reflected in the general criminal framework. The maximum penalties prescribed for this category are imprisonment from ninety-one days to one year and a fine ranging from five million to twenty million rials (6).

Chapter Five concerns the offenses of defamation and the dissemination of falsehoods through computer systems.

In Chapter Six, the legislator specifies the criminal liability of natural and legal persons, including companies providing access services, and treats failure to meet statutory requirements as an offense, even prescribing penalties such as fines up to one billion rials and temporary suspension of operations. Since the services of such companies play a significant role in controlling cybercrimes, and failure to observe legal and ethical standards—such as filtering unethical websites—may impose substantial material and moral harms on society, the legislator has established comparatively stringent enforcement guarantees for this category. In addition, this chapter creates a working group tasked with identifying criminal content in cyberspace, chaired by the Prosecutor General, which convenes twice monthly to review filtering instances. This committee is required to submit a report every six months on the status of criminal-content filtering cases to the heads of the three branches of government and the Supreme National Security Council (11, 12).

Chapter Seven provides for matters such as the distribution and dissemination of viruses, software trafficking, and instruction in system sabotage, and prescribes penalties of imprisonment from ninety-one days to one year and a fine ranging from five million to twenty million rials (1).

Chapter Eight, as the final part of Part One, treats certain circumstances as grounds for sentence aggravation, including where the offender is a government employee, a member of the armed forces, a judicial authority, or, more broadly, holds official or unofficial membership within the three branches of government and commits a computer crime in connection with official duties. It also treats recidivism beyond two occasions as an aggravating

circumstance, requiring the offender to be sentenced to more than two-thirds of the maximum of one or two punishments prescribed by the statute (13).

In Part Two, the legislator specifies the criminal procedure regime for dealing with computer crimes. It begins by addressing the territoriality principle and offenses against the sovereignty of the Islamic Republic of Iran, then continues with provisions on the preservation of digital evidence, and the search and seizure of computer systems by law enforcement officers. It also defines the duties of Internet service providers in preserving computer data and information. In addition, law enforcement officers are required to respect individuals' privacy, and penalties are prescribed where an officer fails to act in accordance with judicial orders. In general, it can be stated that, from a statutory standpoint, no major legal deficiency exists in the area of addressing cybercrimes; however, with respect to certain offenses—such as crimes against chastity and public morality, or the dissemination of computer viruses—relatively lenient punishments have been prescribed. Given the expansive nature of cyberspace and the scale of harms that may result, proportionality between the offense and punishment should be observed and the penalty framework reconsidered (3, 4).

Finally, it is noteworthy that cybercrime cases in Tehran are examined by the Specialized Prosecutor's Office for Combating Computer Crimes, and it is hoped that, through the efforts of responsible authorities, similar prosecutor's offices will be established in other parts of the country as well.

The Concept of Legislative Criminal Policy in the Prevention of Cybercrimes

The emergence of the term "criminal policy," introduced by Feuerbach, a German jurist at the end of the eighteenth century, is closely connected with a rational and wisdom-oriented approach to dealing with crime and is essentially a product of such thinking. The term "policy," which conveys notions of deliberation, guidance, and purposiveness, when combined with the specific meaning attributed to "criminal policy," has led to the acceptance and widespread use of this concept in contemporary legal and sociological discourse. Similar to the use of terms such as "economic policy" and "cultural policy," one of the most important components of Iran's criminal policy in preventing computer crimes is legislation in this field. Cyber legislation can be explained through a three-stage approach.

Legislation in the field of criminal law methods must begin with an understanding of the application of new technologies. Specialized sections, along with security and law enforcement structures—or, in general terms, the police—are required to possess the necessary conditions for investigating cybercrimes. Laying the foundation for effective legislation requires comparing existing criminal laws with the needs arising from new forms of criminal conduct. In many cases, existing laws may be capable of covering new manifestations of traditional crimes.

The third stage involves the drafting of new laws. Based on experience, it may be difficult and challenging for legislative authorities to implement the process of drafting cybercrime laws without international cooperation, due to the rapid growth of network technologies and their complex structures. Drafting cybercrime legislation in isolation may lead to conflicts of laws and a waste of resources. Moreover, monitoring and aligning with the development of international strategies and standards is essential. On this basis, computer crimes may be categorized, on the one hand, as crimes against persons, property, and public security and order, and, on the other hand, as software crimes, data crimes, and crimes against individual private rights. Accordingly, in order to prevent computer crimes, Iran's criminal policy in the field of legislation seeks to prevent the commission of offenses by both potential and actual offenders through the enactment and codification of laws in this domain.

With the growth of computer crimes and emerging offenses in the contemporary era, the police, as one of the effective pillars of the country's judicial policy, have undertaken reforms and transformations in their organizational structure. In this regard, in order to create security in the space of information production and exchange, and alongside reforms in security and law enforcement structures—namely the establishment of the Police of the Production and Exchange of Information—under the second strategy of the National Strategic Document on the Security of the Production and Exchange of Information Space, approved by the Council of Ministers on 26 February 2000, specific responsibilities were assigned to the Law Enforcement Force of the Islamic Republic of Iran.

Conclusion

From this article, it is concluded that computer crimes, like other crimes, consist of the three essential elements of legality, mens rea, and actus reus; that is, the realization of such crimes requires the presence of all three elements. Among these elements, the legal element is more controversial. It has been shown that most countries have been compelled to enact legislation concerning such crimes, and some have even proceeded to amend those newly enacted laws. Based on the arguments presented in the text, it is concluded that the law must clearly define the necessary regulations regarding computer crimes. At first glance, it may appear that attacks against hardware fall outside the scope of computer crimes; however, hardware without data and software is of minimal significance. Moreover, hardware executes programs, processes data, and serves as a repository for them. From this perspective, it must be considered within the discussion of computer crimes. Nevertheless, what most offenders primarily target are data and programs. Therefore, programs, as the principal objects of offenders' attention, require particular care and attention from the legislator.

A portion of computer crime perpetrators consists of specialists and technical experts whose objectives are not genuinely criminal; rather, the outcomes of their actions often lead to discovery and innovation. It is an established fact that technological capabilities have enabled countries to access data located in other states; in other words, from a technical standpoint, access to such data is unavoidable. Accordingly, instead of prohibiting access to data, it should be regulated and governed by rules. Such regulation essentially reconciles the necessity of research with the sovereignty of the state that owns the data. Consequently, countries—particularly those with greater social and economic dependence on cyberspace—have moved toward enacting or reforming criminal laws in this area. In Iran as well, awareness of this dependence on cyberspace is increasing daily. Therefore, Iranian law must move toward enacting or revising criminal legislation to protect the security of data and computer systems of users, governmental bodies, public institutions, and private entities, thereby ensuring the security of data and computer networks and, ultimately, promoting the country's social and economic development in the cyber environment.

Recommendations and Strategies

Cybercrimes require transnational and cross-border cooperation by police forces and judges. Coherent and separate legislation for cybercrimes must be drafted and guaranteed, encompassing substantive and procedural international dimensions, as well as criminal sanctions for matters such as copyright protection and data protection. Police officers and judges must receive specialized training; such training for police should begin from the outset of military education, and specialized cybercrime police units should exist for each specific cyber offense. For example, there should be specialized police units for cyber fraud and cyber forgery, and correspondingly, specialized judges should also be in place.

Specialized units for combating computer and cybercrimes within law enforcement forces, intelligence services, the Ministry of Defense, and armed forces command structures must be equipped with up-to-date and necessary technology. Where such units do not yet exist, they should be established and equipped as a priority. Given that information and communication technologies have created new spaces for offenders, policymakers and administrators must develop legal and executive solutions to address this challenge. To control computer crimes at the global level, it is essential that countries adopt enacted legislation and strive for convergence of laws to the greatest extent possible. In this regard, the creation of a global model appears necessary.

Public participation, particularly from the private sector, strongly reinforces the enforcement of laws and the implementation of educational programs. Computer crime laws and national public education programs in various countries are formulated by councils composed of scientific, industrial, commercial, security, and service organizations. In many countries, entities known as centers for the protection of critical information systems and computer emergency response centers are active. These centers receive scientific support from faculties of electrical engineering, computer science, and law, and financial and political support from defense and security organizations. Governments, in addition to creating legal, executive, and judicial frameworks for addressing computer crimes, are obliged to ensure the proper flow of information among governmental organizations, criminal policymakers, and the private sector. Among the most critical responsibilities of governments is the promotion of a culture of ethical conduct in life and work within the new information environment.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Responses (Update). Geneva: International Telecommunication Union (ITU); 2014.
2. Hosseinikhah. Police and Computer Crimes. Tehran: NAJA Training and Education Deputy Publications; 2011.
3. Gercke M. Understanding Cybercrime: A Guide For Developing Countries. Geneva: International Telecommunication Union (ITU); 2009.
4. Council of Europe. Convention on Cybercrime (ETS No. 185). Budapest: Council of Europe; 2001.
5. Council of Europe. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). Strasbourg: Council of Europe; 2003.
6. Council of Europe. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (ETS No. 201). Lanzarote: Council of Europe; 2007.
7. Council of Europe, editor Criminological Aspects of Economic Crime. Proceedings of the Twelfth Conference of Directors of Criminological Research Institutes; 1976; Strasbourg: Council of Europe.
8. International Telecommunication Union. Resolution 149: Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies. Antalya: ITU Plenipotentiary Conference, 2006.
9. Interpol. Resolution: 6th International Conference on Cybercrime. 2006.
10. Council of Europe Committee of Ministers. Recommendation No. R (89) 9 on computer-related crime. Council of Europe, 1989.
11. Council of Europe Committee of Ministers. Recommendation No. R (87) 15 regulating the use of personal data in the police sector. Council of Europe, 1987.
12. Council of Europe Committee of Ministers. Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services. Council of Europe, 1995.
13. Council of Europe Committee of Ministers. Recommendation No. R (95) 13 concerning problems of criminal procedure connected with information technology. Council of Europe, 1995.