How to cite this article:
Rezaei, M. A., Tadayyon, A., & Esmaeili, M. (2027). Criminological Analysis of Privacy Violations in Cyberspace: A Comparative Study of the Legal Systems of Iran and Afghanistan. *Journal of Historical Research, Law and Policy, 5*(4), 1-15. https://doi.org/10.61838/jhrlp.366

Article history:
Original Research

Dates:
Submission Date: 08 April 2026
Revision Date: 04 July 2026
Acceptance Date: 12 July 2026
First Publication Date: 13 July 2026
Final Publication Date: 01 July 2027

Criminological Analysis of Privacy Violations in Cyberspace: A Comparative Study of the Legal Systems of Iran and Afghanistan

1. Mohammad Aref. Rezaei [1] : Ph.D. student, Department of Political Science, CT.C., Islamic Azad University, Tehran, Iran
2. Abbas. Tadayyon [2*]: Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran
3. Mahdi. Esmaeili [3]: Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

*corresponding author's email: ab.tadayyon@iau.ac.ir

ABSTRACT

The present study was conducted with the aim of providing a criminological analysis of privacy violations in cyberspace from a comparative perspective within the legal systems of Iran and Afghanistan. The central research question examines the extent to which the existing legal frameworks in the two countries are aligned with contemporary criminological principles in addressing cybercrimes against privacy. The study employs a descriptive–analytical methodology with a comparative research approach, and data were collected through the analysis of legal texts, international instruments, and a review of relevant scholarly literature. The findings indicate that although both legal systems have undertaken efforts to criminalize infringements upon digital privacy, these efforts suffer from definitional ambiguities, limited enforcement capacity, and a predominantly reactive approach. Iran, through the Computer Crimes Act of 2009, demonstrates a relatively more developed legislative framework, whereas Afghanistan remains in the early stages of developing its cybersecurity legal structure. The study concludes that integrating preventive criminological approaches with the principles of Islamic jurisprudence can provide a solid foundation for reforming the legal systems of both countries.

Keywords: *Cyber Criminology, Digital Privacy, Comparative Law, Iran, Afghanistan, Cyberspace, Computer Crimes*

Introduction

In recent decades, the digital revolution has transformed the face of the world, and cyberspace has become a platform for billions of citizens. However, alongside these developments, emerging forms of infringement upon fundamental human rights, including privacy, have appeared in this space. The violation of digital privacy, as a serious phenomenon, has attracted the attention of criminologists, jurists, and policymakers across the world. Islamic countries, including Iran and Afghanistan, with a combination of religious values, cultural traditions, and the requirements of legal modernization, are attempting to find an appropriate response to this global challenge. The fact that Islamic jurisprudence has spoken for centuries about respect for privacy places these countries in a distinctive position, in which they possess both rich religious resources and the challenges of modernization (1).

Criminology, as the science that studies crime, the offender, and society's response to crime, provides useful and diverse tools for analyzing cybercrimes. Routine activity theory (2), rational choice theory, and differential association theory (3) each explain, from a different perspective, why and how cybercrimes against privacy occur. Jaishankar (4), by introducing "cyber criminology" as an independent field, demonstrated that cyberspace, due to its distinctive features—borderlessness, anonymity, and speed of dissemination—requires its own specific theoretical and methodological frameworks. Drawing on these frameworks, the present study conducts a comparative analysis of the laws and legal structures of Iran and Afghanistan in order to clarify the position of each country in confronting these emerging threats (5).

The necessity of conducting this study arises from several considerations. First, the existing Persian-language scholarly literature on the comparative criminological analysis of digital privacy violations is very limited. Second, previous studies have mainly focused on a single country and have neglected the comparative approach. Third, criminological dimensions, compared with purely legal dimensions, have not been sufficiently addressed in the existing literature. By seeking to fill these gaps, the present study aims to provide a more comprehensive picture of the status of cyber privacy violations in the two legal systems and to propose solutions based on scientific evidence. The main research question is as follows: To what extent are the existing legal frameworks in Iran and Afghanistan compatible with modern criminological principles in combating cybercrimes against privacy? (6).

The present study is organized into six main sections. Following the introduction, the theoretical and conceptual foundations of digital privacy and related criminological theories are discussed. The research methodology is then explained. The fourth section presents a comparative analysis of the Iranian legal system. The fifth section is devoted to the analysis of the Afghan legal system. The sixth section presents the comparative analysis and the main findings. Finally, the study concludes with conclusions and recommendations. Each section is built upon a solid foundation of valid scholarly references so that the study possesses the necessary credibility for publication in international journals.

Theoretical and Conceptual Foundations

The Concept of Privacy in the Digital Age

Privacy is one of the most fundamental human rights, recognized in Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966). However, the definition and scope of this right have undergone fundamental transformations in the digital age. Daniel Solove (7) considers privacy not as a single concept, but as "a family of related concepts" that assumes different meanings in different contexts. He presents a four-dimensional taxonomy of privacy violations: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion. This analytical framework is used in examining the laws of Iran and Afghanistan in order to determine which of these domains each law covers.

In Islamic jurisprudence, the protection of privacy holds a central position. The noble verse "Do not spy" (Al-Hujurat: 12), as an explicit prohibition against spying into the affairs of others, provides a religious basis for the protection of privacy. The concepts of "inviolability of the home," "concealment of others' faults," and "inviolability of correspondence" in Islamic jurisprudence all protect privacy from different angles (8). This jurisprudential foundation, which has legal validity in both Iran and Afghanistan, can play an important role in justifying and strengthening laws

protecting digital privacy. However, the main challenge is translating these general jurisprudential principles into precise operational regulations in the field of cyberspace, which requires “digital ijtihad.”

Helen Nissenbaum (9), in the theory of “contextual integrity,” argues that a privacy violation occurs when information is transferred from the context in which it was collected to another context with different norms. This theory is highly suitable for understanding why harm occurs in crimes such as the dissemination of private images: the same image that is not harmful within an intimate relationship becomes severely damaging after being disseminated in the public sphere. In the cultural context of Iran and Afghanistan, where honor-related values are strong, this harm has much deeper social dimensions. The laws of the two countries must take this cultural reality into account in criminalization and sentencing.

Relevant Criminological Theories

Routine activity theory, proposed by Cohen and Felson (2), is highly useful for analyzing cybercrimes against privacy. This theory considers the occurrence of crime to be conditional upon the convergence of three elements: a motivated offender, a suitable target, and the absence of a capable guardian. In cyberspace, all three elements are abundantly present: potential offenders have access to numerous targets through the Internet, users’ personal information constitutes a suitable target, and inadequate supervision on platforms removes the “capable guardian” from the equation. This analysis suggests that prevention strategies should focus on reducing access to targets and strengthening guardianship.

Sutherland’s differential association theory (3) explains why some individuals, in online environments where antisocial norms are prevalent, tend to commit cybercrimes. When, within an online group, the dissemination of others’ private images is redefined as “legitimate revenge,” the likelihood of such behavior increases. This theory emphasizes the importance of countering criminal norms in online spaces. In Islamic countries, religious values can function as “counter-norms” against these criminal definitions; Islamic rulings regarding the prohibition of spying and dishonoring others can serve as powerful deterrents (1).

Hirschi’s social control theory (10) introduces four social bonds that deter crime: attachment, commitment, involvement, and belief. In the cyber domain, the weakening of these bonds in the digital environment—where anonymity may reduce the sense of accountability—can lead to an increase in cybercrimes. For Islamic countries, “belief” in religious values is one of the strongest factors of control and must be considered in designing prevention policies. Moreover, Becker’s labeling theory (11) draws attention to the phenomenon of “secondary victimization,” in which victims of honor-related cybercrimes in countries with strong honor-related values suffer more from this phenomenon than victims in Western societies.

Digital Privacy and Islamic Jurisprudence: A Theoretical Link

Islamic jurisprudence, as the main source of legislation in Iran and Afghanistan, contains rich principles that explicitly protect individuals’ privacy. In verse 12 of Surah Al-Hujurat, the Holy Qur’an states: “O you who have believed, avoid much suspicion. Indeed, some suspicion is sin. And do not spy.” This verse, which is frequently cited in the legal literature of both countries, provides a strong Qur’anic foundation for the protection of privacy. In Hanafi jurisprudence, the school followed by the majority of Afghan Muslims, “hurmat al-Muslim” (the dignity and inviolability of the Muslim) functions as a general principle prohibiting any violation of the dignity, secrets, and private

life of Muslims. This principle can serve as a comprehensive jurisprudential basis for criminalizing a broad range of cybercrimes against privacy (8).

The rule of "no harm and no reciprocating harm," one of the most important jurisprudential maxims, provides another basis for protecting digital privacy. This rule, derived from the Prophetic hadith "There shall be no harm and no reciprocating harm in Islam," establishes that neither causing harm to others nor suffering harm from others is permissible in Islam. Digital privacy violations, ranging from the dissemination of private images to identity theft, clearly fall within the scope of this rule. Furthermore, the principle of "blocking the means" in Maliki jurisprudence and the principle of precaution in Imami jurisprudence can provide a basis for preventing cybercrimes before they occur. Integrating these jurisprudential principles with modern criminological frameworks creates an indigenous Islamic approach that possesses both religious legitimacy and scientific validity.

The main challenge in utilizing this jurisprudential capacity is the "implementation gap." Although clear jurisprudential principles regarding privacy exist, their translation into specific and enforceable regulations in the digital domain has not yet been fully accomplished. This task, known in the science of Islamic legal theory as "ijtihad," requires specialists who possess deep knowledge of both jurisprudence and information technology. In Iran, some religious scholars and jurists have begun this effort, but the necessary scholarly consensus has not yet been reached. In Afghanistan, this process is at an earlier stage. Establishing "digital jurisprudence commissions" that bring together religious scholars and cyber law specialists can help close this gap.

"Maqasid al-Sharia," or the objectives of Islamic law, which in Islamic legal theory refer to the preservation of the five necessities of religion, life, intellect, lineage, and property, provide a suitable framework for determining priorities in cyber criminal policy. Cybercrimes against privacy can harm all five necessities: the dissemination of false religious content harms "religion"; cyber threats and intimidation harm "life"; misleading information harms "intellect"; honor-related cybercrimes harm "lineage" and "honor"; and digital fraud damages "property." This jurisprudential framework, which covers all dimensions of cyber harm, can be used as an "Islamic digital rights charter" in the legislation of both countries (12).

Victimology of Cyber Privacy Crimes

Victimology, as a branch of criminology that focuses on victims of crime, offers valuable insights into the nature of harms caused by cybercrimes against privacy. A distinctive feature of the victims of these crimes is their "invisible victimization." Unlike victims of physical crimes, who suffer visible material harm, victims of cybercrimes often face psychological, social, and reputational harms that are less visible but may be more long-term and deeper than physical injuries. Studies show that victims of non-consensual intimate image sharing often suffer from post-traumatic stress disorder, depression, and social anxiety, which sometimes lead to complete isolation (13).

In countries with strong honor-related values, such as Iran and Afghanistan, the social harm caused by honor-related cybercrimes has specific dimensions. "Secondary victimization," in which the victim, after the occurrence of the crime, is also judged and blamed by society, is one of the serious challenges in both countries. This phenomenon, which corresponds with the concept of "labeling victimization" in Becker's theory (11), causes many victims to refrain from reporting the crime. This "underreporting," which conceals the real statistics of cybercrimes in both countries, results in the "dark figure of crime," one of the greatest statistical challenges in the field of cybercrime. Cultural reform, in which the victim is seen not as guilty but as an injured person deserving support, is essential for both systems.

Gendered patterns of victimization in cybercrimes against privacy indicate structural inequalities. International data consistently confirm that women, especially young women, are more frequently targeted than men by crimes such as non-consensual intimate image sharing, digital sexual extortion, and cyber harassment. This gendered pattern, which is also confirmed in Iran and Afghanistan, is rooted in power inequalities, social restrictions, and cultural expectations. The theory of gender-based violence, emphasized by the United Nations in various documents, defines this pattern as structural discrimination requiring a targeted policy response. Both countries must pay explicit attention to this gendered dimension in their laws and policies.

The “cycle of victimization” in cyberspace has features that distinguish it from traditional victimization. First, harm in cyberspace is “permanent”: published content may remain accessible for months or years after dissemination. Second, harm is “widespread”: a post on a social network can reach millions of people within seconds. Third, harm is “replicable”: content can be repeatedly redistributed by different individuals. These three features, which do not exist in traditional crimes, show that traditional criminal responses are insufficient to reduce harm to victims. “Immediate content removal mechanisms,” which are now incorporated into cyber laws in advanced countries, are among the most essential tools for reducing this permanent harm (7).

Methodology

This study is descriptive–analytical in nature and adopts a comparative legal research approach. Data were collected through library research, and the sources include primary legal texts, including the constitutions, penal laws, and cyber regulations of the two countries; international legal instruments, including the Budapest Convention of 2001 and the United Nations Declaration of 2013; and valid scholarly literature published in peer-reviewed journals. The unit of analysis is the “legal system” in each country, examined from legislative, judicial, and executive dimensions. For comparative evaluation, seven specific criteria were designed: (1) legislative coverage; (2) definitional precision; (3) proportionality of sanctions; (4) institutional capacity; (5) judicial practice; (6) international compatibility; and (7) attention to the cultural–religious context. The method of triangulation was used to enhance the validity of the findings (14).

The comparative approach of this study is inspired by the framework of Zweigert and Kötz (15), which emphasizes “functional comparison” rather than merely “formal comparison.” This means that the study assesses not only the texts of laws, but also their practical effectiveness in confronting digital privacy violations. To avoid “ethnocentric evaluation,” an effort has been made to evaluate each legal system within its own specific context, considering its history, culture, and sources. The main limitation of the study is limited access to codified judicial practice in both countries, which makes the analysis more inclined toward written laws. Nevertheless, reference to reports from Iran’s Cyber Police, UNODC statistics, and existing field studies has partially compensated for this limitation.

Criminological Analysis of the Iranian Legal System

Constitutional Foundations

Article 22 of the Constitution of the Islamic Republic of Iran (1979, amended in 1989) states: “The dignity, life, property, rights, residence, and occupation of persons are immune from violation, except in cases prescribed by law.” Article 25 also explicitly protects freedom of communications and correspondence. From a criminological perspective, these constitutional guarantees show that the Iranian state is, in principle, obligated to protect citizens’

privacy. However, the absence of an “explicit right to digital privacy” in the Constitution, which could be invoked without the need to prove material harm, is one of the fundamental gaps in the Iranian legal system. This gap causes victims of cybercrimes against privacy to face greater difficulties in proving their claims (16).

The Computer Crimes Act of 2009

Iran’s Computer Crimes Act, approved on July 27, 2009, with 74 articles, is the main legal instrument for confronting cybercrimes, including privacy violations. Articles 16 to 22 of this law, which are directly related to privacy, address unauthorized access, interception of communications, and dissemination of private information. From the perspective of routine activity theory, this law attempts to increase offenders’ “perceived risk” through criminalization and punishment. However, several serious shortcomings exist: first, “personal data” is not precisely defined; second, emerging crimes such as deepfakes and digital sexual extortion are not covered; third, punishments are not sufficiently deterrent; and fourth, no rapid mechanism exists to stop the dissemination of harmful content (5).

Analysis of existing judicial practices, although limited, shows that Iranian courts face three main challenges in adjudicating cybercrimes against privacy: (1) evaluating and admitting digital evidence; (2) interpreting legal provisions in unprecedented cases; and (3) determining proportionate punishment. From the perspective of social control theory, when punishments are not deterrent for offenders, the primary function of law in strengthening “belief” in the legal order is weakened. Reports from Iran’s Cyber Police indicate that cybercrimes against privacy have increased in recent years, while the proportion of cases resulting in final convictions remains low. This pattern indicates a gap between legislation and enforcement (17).

Criminological Evaluation

From a criminological perspective, the Iranian legal system follows a “reactive” model, in which the response to crime occurs after its commission. This approach, which corresponds with traditional penal models, is insufficient for confronting cybercrimes whose consequences are immediate and widespread. Situational crime prevention theory suggests that by changing the environment and opportunities for crime, crime commission can be made more difficult. From this perspective, Iran has not invested sufficiently in “primary prevention” measures such as digital literacy education and “situational prevention” measures such as requiring platforms to adopt safe design. The main focus has been on “tertiary prevention,” namely punishment after the crime has occurred (16).

Iran’s institutional capacity, compared with developing countries in the region, is relatively better. The Cyber Police, with more than a decade of experience, specialized computer crime courts, and the MAHER Center are among the executive structures established in this field. However, the ratio of specialized personnel to the volume of crimes is inadequate, continuous training for judges and prosecutors is limited, and intersectoral coordination is weak. From the perspective of routine activity theory, this means “ineffective guardians,” which completes the crime triangle. Reforming this institutional capacity is among the most urgent needs of the Iranian legal system in this field.

Emerging Crimes and Legal Gaps in Iran

One of the main challenges of the Iranian legal system is the speed of technological change and the emergence of new crimes that existing laws have not addressed. “Deepfake,” in which artificial intelligence is used to create

realistic synthetic content, is one of these crimes. This technology, initially developed in the entertainment industry, has rapidly become a tool for harming privacy, defamation, and extortion. In Iran, no legal provision explicitly treats deepfakes as an independent crime; courts must rely on general provisions such as forgery or insult, which are not fully appropriate for this phenomenon. Countries such as the United States, South Korea, and the United Kingdom have placed the explicit criminalization of deepfakes on their legislative agendas, which can serve as a model for Iran (18).

"Digital sexual extortion," or sextortion, in which the threat of publishing private content is used for extortion, is another crime that lacks explicit coverage in Iranian law. Existing judicial practices show that judges handle this crime through provisions related to threats and extortion in the Islamic Penal Code, but these provisions were not designed for the specific cyber features of this crime. "Cyberstalking," meaning continuous surveillance of the victim's online activities, is also a crime that existing Iranian laws do not sufficiently cover. "Unauthorized data collection" by technology companies and online platforms also remains without explicit legal regulation. These four crimes, all of which are explicitly criminalized in advanced countries, are urgent gaps in the Iranian legal system that must be addressed.

The challenge of "extraterritorial jurisdiction" is another serious issue that Iran's Computer Crimes Act has not sufficiently addressed. When an offender acts from another country—for example, disseminating the private images of an Iranian victim from a foreign server—prosecution faces serious jurisdictional challenges. In Iran, the Computer Crimes Act establishes initial bases for extraterritorial jurisdiction, but sufficient mechanisms for international cooperation do not exist. The Budapest Convention of 2001, which provides a comprehensive framework for international cooperation in cybercrime, has not yet been ratified by Iran. Accession to this convention or negotiation of similar bilateral agreements is an essential step for increasing the effectiveness of Iran's cyber law enforcement at the international level (5).

"Intermediary liability" is one of the most complex legal issues of the digital age and has not yet been clearly regulated in Iran. What responsibility do platforms such as Instagram, Telegram, and WhatsApp, which transmit hundreds of millions of messages daily, have with respect to content that causes violations of users' privacy? In the European Union, the Digital Services Act of 2022 regulates this responsibility in detail. In Iran, this gap means that platforms are often exempt from responsibility for content disseminated by their users. Designing a framework of "conditional intermediary liability," under which platforms are held responsible if they fail to remove harmful content after receiving notice, is among the necessary reforms for the Iranian legal system (16).

Criminological Analysis of the Afghan Legal System

Legal and Sharia Foundations

The legal system of Afghanistan under the Islamic Emirate is based on the rules of Islamic Sharia. This framework, rooted in Hanafi jurisprudence, in principle provides strong protection for individuals' privacy. Rules such as the prohibition of spying ("Do not spy"), the prohibition of backbiting, and the inviolability of correspondence can be invoked both as religious duties and as a foundation for cyber legislation (12). This jurisprudential capacity, which is shared with Iran but plays a more central role in Afghan legislation, can serve as a strong source of legitimacy for protecting digital privacy. The main challenge is "digital ijtihad," meaning the derivation of specific

jurisprudential rulings for emerging issues in cyberspace, which requires cooperation between religious scholars and legal specialists.

Penal Code and Cyber Regulations

The Penal Code of Afghanistan, approved in 2018, covers a range of cybercrimes in Chapter Five, Articles 459–488. Article 462 criminalizes unauthorized access to systems, and Article 465 criminalizes unauthorized interception. However, compared with Iran's Computer Crimes Act, these provisions are less comprehensive and less specialized. The absence of an independent cybercrime law, the lack of a precise definition of "personal data," and the absence of explicit criminalization of digital sexual extortion are among the most important gaps. From the perspective of rational choice theory, when the probability of arrest and punishment is low, offenders assess the benefits of crime as greater than its costs. In Afghanistan, both the probability of arrest and the severity of punishment lack the necessary level of deterrence (16).

Afghanistan's institutional capacity is at an earlier stage compared with Iran. The absence of an equipped specialized cyber police unit, the shortage of judges trained in computer crimes, and the low level of digital literacy among judicial officials are among the main executive challenges. However, one unique advantage of Afghanistan is the extensive network of mosques and religious schools, which can play an effective role in public education about the prohibition of spying and respect for others' privacy. This capacity, which has not yet been properly used, can be employed as part of a value-based Islamic "primary prevention" strategy (5).

Opportunities and Capacities in Afghanistan

Despite the numerous challenges of Afghanistan's legal system, valuable opportunities and capacities also exist that have not yet been properly utilized. The first opportunity is the extensive network of mosques and religious schools, which can function as a "parallel educational network" for promoting Islamic digital ethics. Friday and congregational prayer leaders, who in many villages are the only informed authorities in the community, can transmit messages about the prohibition of spying, the prohibition of digital dishonoring, and support for victims. This approach, if supported by specific fatwas from religious scholars, may be more effective than formal laws because it relies on people's inner belief rather than merely on fear of punishment (12).

The second opportunity is Afghanistan's young generation, which is using the Internet more rapidly than the previous generation. This generation, among whom Internet penetration is growing faster than in other age groups, is both the most important target of digital literacy education and can become the main driver of changing social norms regarding digital privacy. Educational programs that teach digital privacy within the framework of Islamic values—for example, "respecting others' privacy is a sign of faith"—can be more influential among young people. The successful experience of some Islamic countries, such as Malaysia, in incorporating digital ethics into school curricula can serve as a suitable model for Afghanistan.

The third opportunity is the capacity for international cooperation. Organizations such as UNODC, Interpol, the International Telecommunication Union, and the Organization of Islamic Cooperation have specific programs for developing the cyber capacity of developing countries. Afghanistan can use these programs to train specialized human resources, equip cyber police units, and develop appropriate laws. The fourth opportunity is cooperation with Iran. These two countries, with shared language, culture, and religion, possess ideal conditions for cooperation in the cyber domain. Iran, with more than a decade of experience in implementing computer crime laws, can provide

models, lessons learned, and even practical training for Afghanistan. This cooperation, which is still at an informal stage, should be transformed into a formal “cyber cooperation agreement” with a specific legal framework.

The fifth opportunity is the “clean slate” that Afghanistan has compared with Iran. Iran, with several decades of cyber legislation experience, faces a complex “legislative legacy,” the reform of which is more difficult than building from the beginning. Afghanistan can design a cybercrime law from scratch, learn from the mistakes and shortcomings of Iran and other countries, and create a more comprehensive, more coherent, and more suitable framework for its own conditions. This “late mover advantage,” known in the literature of economic development, also applies to the field of legislation. By properly using this opportunity, Afghanistan can surpass Iran in cyber legislation, provided that the necessary political will exists.

Comparative Analysis and Discussion

Comparison Based on the Seven Criteria

Evaluation of the two systems based on the seven criteria of the study shows the following results: in the criterion of “legislative coverage,” Iran, due to the existence of a specialized computer crimes law, is in a better position, which is relatively adequate, whereas Afghanistan relies only on general provisions of the Penal Code, which is inadequate. In the criterion of “definitional precision,” both countries face serious ambiguities in defining key concepts such as “personal data” and “consent,” which is inadequate. In the criterion of “proportionality of sanctions,” the punishments in both countries lack sufficient deterrence for serious crimes such as digital sexual extortion. In the criterion of “institutional capacity,” Iran is more advanced, but both face a shortage of specialists. In the criterion of “judicial practice,” Iran has more experience. In the criterion of “international compatibility,” neither country is fully aligned with the Budapest Convention or the GDPR. Finally, in the criterion of “attention to the religious–cultural context,” both countries possess high jurisprudential capacity that has not yet been properly used in cyber legislation (6).

From a criminological perspective, the most important common feature of the two systems is the dominance of a “reactive–penal” approach over a “preventive–comprehensive” approach. Both systems mainly focus on punishment after the occurrence of crime and have neglected sufficient investment in primary prevention, including education; secondary prevention, including identification and early intervention; and tertiary prevention, including victim support. This is while, in cyberspace, crime often occurs at high speed and with widespread effects, and punishment after the occurrence of crime usually cannot fully compensate the harm suffered by the victim. In honor-related privacy violations, these harms may be permanent and irreparable (19).

Shared Capacities and Development Opportunities

The findings of this study show that both countries possess valuable shared capacities that have not yet been properly used. First, Islamic jurisprudential foundations, which explicitly prohibit spying, dishonoring others, and violating others’ secrets, can be framed as “Islamic digital ethics” and can enjoy higher legitimacy and social acceptance than purely positive laws. Second, bilateral cooperation between Iran and Afghanistan in the field of cybercrimes, benefiting from the historical, cultural, and linguistic links between the two countries, can be effective in confronting transnational cybercrimes. Third, the participation of religious scholars in both countries in designing and promoting digital privacy standards can have an influence beyond formal laws.

Case Analysis: Non-Consensual Dissemination of Private Images

To demonstrate the practical application of the theoretical framework of this study, a case analysis of "non-consensual dissemination of private images" in the two legal systems is useful. This crime, which is one of the most common cybercrimes against privacy in both countries, provides a clear example of the gap between law and reality. In Iran, this crime is mainly addressed through a combination of Article 17 of the Computer Crimes Act and Article 694 of the Islamic Penal Code, concerning violation of dignity. However, this combination, resulting from the absence of independent and precise criminalization, creates several problems: first, determining which provision should be applied depends on the judge, leading to inconsistency; second, the elements of the crime, such as "consent" and "privacy," are not clearly defined in either provision; third, the prescribed punishments under these two provisions differ, which can lead to unjust outcomes in similar cases (1).

In Afghanistan, this crime lacks even clearer legal coverage. Courts must rely on general provisions such as "promotion of immorality" or "violation of dignity" in the Penal Code, which were essentially designed for different contexts. This means that, in many cases, precise correspondence between the reality of the cybercrime and the existing legal elements is difficult. From the perspective of the principle of legality, which in Islamic jurisprudence is also known as the principles of "presumption of innocence" and "no crime without textual authority," this situation is concerning: Can a person be convicted for conduct that had not been explicitly criminalized at the time of commission? This fundamental question creates a serious challenge for the courts of both countries in NCII cases and shows that the explicit criminalization of this behavior is not only desirable but also necessary from the perspective of criminal law principles (5).

From the perspective of routine activity theory, analysis of this crime shows that all three elements of the crime triangle are clearly identifiable. The "motivated offender" is often the victim's former intimate partner, whose motivation may be revenge, control, or harm. The "suitable target" consists of images or videos created during the relationship with the victim's implied consent but never intended for public dissemination. The "ineffective guardian" includes the absence of technical mechanisms to prevent resharing of content, weakness in user education regarding the secure storage of private content, and the slow response of platforms to takedown requests. Intervention in all three elements—for example, through "right to immediate takedown" laws, education about healthy relationships, and requiring platforms to respond quickly—can have significant effectiveness.

The implications of this case analysis for policymaking are clear. Both countries should: (1) criminalize NCII as an independent offense with a precise definition; (2) determine punishments proportionate to the harm caused, including fines, imprisonment, and compensation; (3) create an "emergency takedown" mechanism for published content that can be implemented within 24 to 48 hours; and (4) support the destigmatization of victims through public education and training for police and judges. This case shows how precise criminological analysis can lead to the design of specific and operational policies, which is the objective that this study has pursued from the outset (19).

Limitations of the Study and Directions for Future Research

This study, like any scientific study, faces limitations that should be considered in interpreting the findings. The first limitation is limited access to published judicial decisions in both countries, which has directed the analysis toward legal texts and limited the "practical" dimension of the analysis. The second limitation is the absence of

reliable official statistics on the real rate of cybercrimes against privacy, which makes quantitative evaluation of policy effectiveness difficult. The third limitation is the dynamic nature of the subject: new technologies such as generative artificial intelligence are evolving at a speed that may require some findings to be reconsidered in the near future. These limitations are not methodological weaknesses, but rather the reality of conducting research in an emerging and rapidly evolving field (17).

Several paths are proposed for future research. First, empirical studies through interviews with judges, lawyers, cyber police officers, and victims can provide richer qualitative data on the real experience of these crimes. Second, content analysis of judicial cases, if access becomes possible, can clarify patterns of judicial practice more clearly. Third, broader comparative studies that also include other Islamic countries, such as Malaysia, Indonesia, Saudi Arabia, and the United Arab Emirates, can identify successful models. Fourth, interdisciplinary research linking criminology with computer science and artificial intelligence is essential for better understanding emerging crimes such as deepfakes. Fifth, the development of an "Islamic Digital Privacy Index," which could quantitatively measure the effectiveness of the legal systems of Islamic countries in this field, could serve as a valuable tool for future comparative research (6).

One of the emerging research areas to which this article only briefly refers is the relationship between generative artificial intelligence and digital privacy in Islamic countries. Tools that can produce realistic images, voices, and texts create new challenges for the concepts of "consent" and "authenticity." In Islamic jurisprudence, the concepts of "testimony" and "evidentiary proof" may require reconsideration in an era in which every image and voice can be fabricated. These fundamental questions, located at the intersection of jurisprudence, technology, and law, provide a rich research field for future scholars, and Iran and Afghanistan, with their rich jurisprudential heritage, can be active participants in this global discourse.

Proposal for an "Islamic Cyber Criminology" Framework

One of the important findings of this study is the need to develop a new theoretical framework that can be called "Islamic Cyber Criminology." This framework, which is still in the early stages of development, seeks to combine Western criminological theories, including routine activity theory, differential association theory, and social control theory, with jurisprudential concepts such as inviolability, honor, maqasid al-Sharia, dar', and ta'zir. Such a framework has three advantages: first, scientifically, it enables a more precise analysis of cybercrimes in Islamic contexts, which purely Western frameworks are unable to provide. Second, from a policy perspective, reform proposals based on this framework will enjoy higher social–religious legitimacy. Third, from an educational perspective, it can serve as the basis for new curricula in universities of Islamic countries that train a new generation of cyber law specialists.

The main elements of this proposed framework are as follows: (1) the "principle of digital inviolability," derived from the jurisprudential concept of "hurmat al-Muslim," which introduces individuals' digital dignity as a fundamental right; (2) the "principle of intensified non-spying," which extends the Qur'anic principle of "do not spy" to the digital sphere and limits any unnecessary surveillance, whether by individuals or by states; (3) the "principle of balance among objectives," which, based on maqasid al-Sharia, establishes a balance between collective security and individual privacy; and (4) the "principle of reform orientation," which, inspired by the concept of repentance in Islamic jurisprudence, emphasizes the rehabilitation of young offenders rather than mere punishment. These four

principles can form the pillars of a comprehensive theoretical framework for future cyber criminology research in the Islamic world (8).

Policy Implications for International Cooperation

The findings of this study have specific implications for the position of Iran and Afghanistan in the international discourse on digital rights. Both countries, despite their internal challenges, can play a more active role in shaping international norms of digital privacy from an Islamic perspective. At present, most international digital privacy frameworks, including the GDPR and the Budapest Convention, have been developed by Western countries and do not sufficiently reflect the perspectives of the Islamic world. This gap provides an opportunity for Islamic countries, including Iran and Afghanistan, to amplify the voice of the Islamic world in this international discourse through the Organization of Islamic Cooperation or other regional institutions (19).

Active participation in institutions such as the Internet Governance Forum, which is held annually, is one of the existing opportunities. This forum, which provides a platform for multi-stakeholder dialogue on Internet issues, can serve as a venue for presenting Islamic perspectives on digital privacy. Moreover, participation in specialized United Nations working groups on privacy in the digital age provides an opportunity for Iran and Afghanistan to share their experiences—both challenges and indigenous solutions—with the international community. This participation not only helps improve the international standing of these countries but can also lead to mutual learning and access to international technical and financial resources.

From the perspective of "science diplomacy," academic cooperation among research institutions in Iran, Afghanistan, and other Islamic countries in the field of cyber law can lead to the creation of an "epistemic community" that, over time, influences national and international policymaking. Successful examples of this approach in other fields, such as scientific cooperation among Islamic countries in the field of Islamic banking, which led to the creation of accepted international standards, show that this path is possible. Establishing an "Islamic Cyber Law Research Network" with the participation of universities from Iran, Afghanistan, Malaysia, Indonesia, and other interested countries can be the starting point of this process (6).

Final Considerations on the Balance between Privacy and Security

At the end of this analysis, it is necessary to address a fundamental tension that has been implicitly present throughout this study: the balance between individual privacy and collective security. This tension, which exists in all legal systems of the world—not only in Iran and Afghanistan—acquires special dimensions in countries facing security challenges. From the perspective of Islamic jurisprudence, this balance can be managed through the concept of maqasid al-Sharia: preserving social security, meaning the preservation of life and religion at the collective level, and preserving individual privacy, meaning the preservation of honor and dignity at the individual level, are both objectives of Sharia, and neither has absolute priority over the other; rather, they must be balanced based on the principle of proportionality (8).

This study argues that strengthening the protection of ordinary citizens' digital privacy against one another—which has been the main subject of this article—is not fundamentally in conflict with the security objectives of the state; rather, it can complement them. When citizens feel that the legal system protects their privacy against cybercriminals, not against the state, their trust in the rule of law increases, which itself is one of the foundations of sustainable security. Therefore, the reforms proposed in this study—more precise criminalization, institutional

capacity-building, and victim support—are not only not in conflict with security objectives, but can also strengthen social security by increasing public trust. This framing of “privacy as security,” rather than “privacy versus security,” can provide a way to overcome existing political tensions in this field and create broader consensus for reform.

This study ends with the message that criminology is, ultimately, a science in service of the human being. The final objective of the criminological analysis of privacy violations in cyberspace is not merely the production of academic knowledge, but the reduction of the suffering of human beings who become victims of these crimes: women whose images have been disseminated without consent, adolescents who have been subjected to cyber harassment, and families whose honor has been harmed due to the misuse of personal information. Iran and Afghanistan, two nations with a rich Islamic–cultural heritage, have the ability to present a model of “Islamic digital justice” that is both rooted in tradition and responsive to the challenges of the twenty-first century. This study hopes to be a small step on this great path.

Conclusion and Recommendations

Through a criminological analysis of privacy violations in cyberspace in the two legal systems of Iran and Afghanistan, this study showed that both countries suffer from common weaknesses: a penal–reactive approach, definitional gaps, weak enforcement capacity, and insufficient use of preventive capacities. At the same time, the shared Islamic jurisprudential foundation and the cultural–linguistic ties between the two countries constitute important unused capacities. The results of this study are consistent with Wall’s findings (13), which documented the dominance of reactive approaches over preventive approaches in developing countries, and with Jaishankar’s findings (4) regarding the necessity of an indigenous theoretical framework for the cyber criminology of non-Western countries.

The practical recommendations of this study are presented along four axes. The first axis is legislative reform through the adoption of a comprehensive data protection law in Iran, an independent cybercrime law in Afghanistan, and the explicit criminalization of emerging crimes such as deepfakes and digital sexual extortion in both countries. The second axis is institutional capacity-building through specialized training for judges and police, the establishment of digital forensic laboratories, and the creation of an independent privacy oversight body. The third axis is the development of a primary prevention strategy through digital literacy education in schools and mosques with content based on Islamic values. The fourth axis is bilateral cooperation in exchanging information about cyber offenders, harmonizing legal definitions, and establishing a joint academic consortium (17).

This study has limitations that must be considered in interpreting the findings: limited access to codified judicial practice, the absence of reliable official statistics, and rapid changes in the technological landscape. For future research, empirical study through interviews with judges, lawyers, and victims is recommended. Moreover, comparison with other Islamic countries, such as Malaysia, Indonesia, and Jordan, which have made significant progress in developing digital law, can provide more practical models. Finally, the development of an “Islamic digital rights framework” inspired by the shared values of the Islamic world is one of the emerging research areas that has not yet received sufficient attention.

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 adhered 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. Abbasi MJ. Cybercrimes and Privacy in Iranian Law. Tehran: Mizan Publications; 2020.
2. Cohen LE, Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review. 1979;44(4):588-608.
3. Sutherland EH. Principles of Criminology. 4th ed: Lippincott; 1947.
4. Jaishankar K. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior: CRC Press; 2011.
5. Hosseini M. Crimes against Privacy in Cyberspace. Tehran: Jangal Publications; 2021.
6. Salehi M. A Comparative Study of Criminal Protection of Privacy in Iranian and American Law. Quarterly Journal of Criminal Law and Criminology. 2022;9(1):79-105.
7. Solove DJ. Understanding Privacy: Harvard University Press; 2008.
8. Kariminia M. Jurisprudential Foundations of Privacy. Islamic Studies Quarterly. 2019;71(1):11-40.
9. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life: Stanford University Press; 2010.
10. Hirschi T. Causes of Delinquency: University of California Press; 1969.
11. Becker HS. Outsiders: Studies in the Sociology of Deviance: Free Press; 1963.
12. Bagherinejad Z. A Jurisprudential Examination of Privacy in the Digital Age. Quarterly Journal of Jurisprudence and Principles. 2020;53(1):1-30.
13. Wall DS. Cybercrime: The Transformation of Crime in the Information Age: Polity; 2007.
14. Saberi F. Legal Analysis of Disclosure of Personal Information on Social Networks. Criminal Law Research Quarterly. 2019;8(2):123-46.
15. Zweigert K, Kötz H. Introduction to Comparative Law. 3rd ed: Oxford University Press; 1998.
16. Alizadeh A. Iranian Criminal Policy toward Privacy Violations in Cyberspace. Tehran: Judiciary Research Institute, 2018.
17. Farahmand S. Challenges of Implementing the Computer Crimes Law in Iran. Legal Critique Quarterly. 2021;4(1):55-78.
18. Rezaeipour N. A Comparative Analysis of Iranian Computer Crime Laws and the Budapest Convention. Judiciary Law Journal. 2021;85(116):23-54.
19. Mousavi Z. Criminal Liability in Unauthorized Disclosure of Private Information. Faculty of Law, University of Tehran. 2020;50(2):100-25.