



University of Tehran Press

Comparative Law Review

Homepage: <https://jcl.ut.ac.ir>

Online ISSN: 2423-3404

Volume: 17, Issue: 1
Spring & Summer
2026

Criminal Protection of Privacy in Iranian and French Law: Comparative Analysis and Proposed Solutions

Razieh Saberi¹ | Sayyad Bigham Barouj²

1. Corresponding Author; Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran. Email: r.saberi@iau.ac.ir
2. Master's Graduate in Criminal Law and Criminology, Department of Criminal Law and Criminology, Tehran Central Branch, Islamic Azad University, Tehran, Iran. Email: 2741705501@iau.ir

Article Info	Abstract
Article Type: Research Article	Detailed Abstract
Received: 2025/08/31 Received in revised form: 2025/10/27 Accepted: 2025/12/11 Published online: 2026/08/23	Introduction and Objective : Privacy is one of the fundamental dimensions of human dignity and personal autonomy. In contemporary legal systems, the protection of privacy has become increasingly significant due to the rapid development of information technologies, the expansion of cyberspace, the widespread use of surveillance tools, and the growing capacity of public and private actors to access, process, and disseminate personal information. From the perspective of criminal law, privacy protection is particularly important because criminal norms are expected to provide the highest level of legal protection against serious and harmful intrusions into individuals' private lives. Despite the universal importance of privacy, legal systems differ considerably in defining its scope, determining its protected interests, criminalizing its violations, and designing enforcement mechanisms. These differences become more visible when comparing legal systems with distinct theoretical, cultural, and institutional foundations. The present study examines the criminal protection of privacy in Iranian and French law through a comparative approach. The main objective is to identify the strengths and weaknesses of both systems, evaluate the adequacy of their criminal responses to privacy violations, and propose legal and institutional solutions for improving privacy protection in Iran. Iran and France have been selected for comparison because they represent two different models of legal development in the field of privacy. Iranian law is influenced by Islamic legal principles, constitutional guarantees, and dispersed statutory provisions, while French law is based on a long-standing civil law tradition, the recognition of privacy as an individual right, and an advanced system of data protection and institutional supervision. This comparison makes it possible to assess how different legal foundations and
Keywords: <i>Criminal Protection, Cyberspace, French Law, Iranian Law, Privacy.</i>	

Article Info

Abstract

enforcement structures affect the real protection of privacy.

Methodology: This research is conducted through a descriptive-analytical and comparative legal method. It examines constitutional provisions, criminal statutes, procedural rules, data protection regulations, doctrinal writings, and relevant institutional practices in Iranian and French law. In the Iranian legal system, the study analyzes constitutional principles, particularly Articles 22 and 25 of the Constitution, as well as provisions of the Islamic Penal Code, the Computer Crimes Law, the Criminal Procedure Code, and other related regulations. In the French legal system, the research focuses on Article 9 of the Civil Code, relevant provisions of the Penal Code, particularly those concerning violations of private life, and the General Data Protection Regulation as applied within the French legal order.

The study also considers practical and institutional dimensions of privacy protection, including the role of judicial authorities, law enforcement bodies, administrative agencies, and independent supervisory institutions. By comparing legal rules and enforcement mechanisms, the research seeks to determine whether the protection granted by law is merely formal or whether it can effectively prevent, control, and punish violations of privacy.

Findings: The findings show that Iranian law recognizes privacy as a protected value, but this recognition has not yet resulted in a coherent and comprehensive criminal protection system. Although the Constitution protects certain aspects of individual security, correspondence, communications, and personal dignity, Iranian legislation does not provide a unified and precise definition of privacy. As a result, the scope of protected private life remains uncertain in many situations, especially in relation to cyberspace, personal data, images, biometric information, vehicles, public places, and digital communications.

Iranian criminal law contains several provisions that may be used to address privacy violations, including rules concerning unlawful access to data, disclosure of secrets, unauthorized surveillance, and violations of communications. However, these provisions are scattered across different laws and do not constitute an integrated system. This fragmentation creates interpretive difficulties for courts and enforcement bodies and weakens the predictability and deterrent effect of criminal law. In addition, the absence of specialized and independent supervisory institutions has limited the effectiveness of privacy protection, particularly in cases involving digital technologies and large-scale data processing.

Another major challenge in Iranian law is the tension between privacy protection and other legal, religious, or security-based considerations. Concepts such as public morality, social order, national security, and the duty of enjoining good and forbidding wrong may, in practice, create broad grounds for interference with private life if they are not precisely defined and judicially controlled. The lack of clear limits on exceptions to privacy protection may lead

Article Info	Abstract
	to inconsistent enforcement and increase the risk of arbitrary or disproportionate interference. Moreover, weaknesses in technical infrastructure, insufficient specialization among some enforcement authorities, and the lack of coherent judicial precedent have further reduced the practical efficiency of existing protections. By contrast, French law provides a more systematic and developed framework for the protection of privacy. Article 9 of the French Civil Code expressly recognizes the right to respect for private life, while the French Penal Code criminalizes several forms of intrusion, including unlawful recording, transmission, or publication of private words or images. In addition, the GDPR and French data protection legislation establish detailed rules concerning the collection, processing, storage, and transfer of personal data. These rules are supported by administrative and criminal sanctions, as well as by institutional oversight. A significant strength of the French system is the role of the National Commission on Information and Liberties, known as CNIL. As an independent supervisory authority, CNIL monitors compliance with data protection rules, investigates violations, issues warnings, imposes sanctions, and contributes to the development of privacy standards in response to technological change. This institutional model has strengthened the practical enforceability of privacy rights and has provided citizens with more effective mechanisms for complaint and redress. Nevertheless, the French system also faces important challenges. The use of modern surveillance technologies, including facial recognition, biometric databases, algorithmic monitoring, and large-scale digital data processing, has created new risks for privacy. These risks are particularly sensitive when justified by public security, counter-crime strategies, or administrative efficiency. Although French law imposes stricter safeguards and judicial or administrative controls, ensuring effective oversight remains difficult in practice due to the speed of technological development and the volume of data processing activities. Therefore, even a relatively advanced legal system must continuously revise its protective mechanisms. The comparative analysis demonstrates that the main differences between Iranian and French law lie in five areas: the clarity of legal definitions, the coherence of statutory protection, the strength of enforcement mechanisms, the existence of independent supervisory institutions, and the limitation of exceptions to privacy protection. While Iran has important normative foundations for recognizing privacy, France has developed a more operational and enforceable model. The French experience shows that privacy protection cannot rely solely on general legal principles; it requires precise legislation, specialized institutions, effective sanctions, transparent procedures, and continuous adaptation to technological developments. Conclusion: The research concludes that improving the criminal protection of privacy in Iran requires comprehensive legislative and institutional reform. First, Iranian law should adopt a clear, inclusive,

Article Info	Abstract
	and practical definition of privacy that covers physical privacy, informational privacy, communications, images, biometric data, digital identity, and personal data in cyberspace. Second, the existing scattered provisions should be integrated into a coherent legal framework capable of addressing both traditional and technology-based violations of privacy. Third, privacy violations should be criminalized with greater precision, especially in relation to unauthorized access to personal data, unlawful publication of images, misuse of smart technologies, illegal biometric data collection, digital surveillance, and disclosure of confidential information. Criminal sanctions should be proportionate, deterrent, and accompanied by administrative and civil remedies. Fourth, exceptions to privacy protection must be clearly defined, narrowly interpreted, and subject to prior or subsequent judicial supervision. Broad and vague references to security, morality, or public interest should not be sufficient to justify interference with private life. Finally, the establishment of an independent supervisory authority for data and privacy protection is essential. Such an institution should have structural and financial independence, investigative powers, authority to impose sanctions, the ability to receive and process citizens' complaints, and a duty to publish transparent reports. The French CNIL can serve as a useful comparative model, provided that it is adapted to the legal, social, and institutional context of Iran. Effective criminal protection of privacy depends on achieving a careful balance between individual freedoms and legitimate public interests. This balance cannot be realized through fragmented laws or purely reactive criminal responses. It requires a preventive, coherent, transparent, and rights-based framework. The French legal experience demonstrates that strong legal definitions, independent supervision, and enforceable sanctions can significantly improve the protection of privacy. Accordingly, Iran can strengthen its legal system by adopting a comprehensive privacy and data protection law, limiting exceptions, reinforcing judicial oversight, and creating an independent supervisory body. Such reforms would contribute to the protection of human dignity, individual freedom, and public trust in the legal system.
How To Cite	Saberi, Razieh; Bigham Barouj, Sayyad (2026). Criminal Protection of Privacy in Iranian and French Law: Comparative Analysis and Proposed Solutions. <i>Comparative Law Review</i> , 17 (1), 173-207. DOI: https://doi.com/10.22059/jcl.2026.396787.634775
DOI	10.22059/jcl.2026.396787.634775
Publisher	The author(s) retain the copyright. 