DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Amirian Farsani, A. (2027). Criminal Management for Protective Support of Free Access to Information with a Perspective on Filtering. *Digital Transformation and Administration Innovation,* 5(2), 1-13.

Received date: 2025-09-06 Revised date: 2025-11-19 Accepted date: 2025-11-26 Initial published date: 2025-11-28 Final published date: 2027-04-01

Criminal Management for Protective Support of Free Access to Information with a Perspective on Filtering

Amin Amirian Farsani[1]*

1. Assistant Professor, Department of Law, Faculty of Humanities Sciences, University of Gonabad, Gonabad, Iran

*Correspondence: amirian_farsani@gonabad.ac.ir

Abstract

Criminal management aimed at protective support for free accessibility to information represents an emerging approach that links the domains of criminal justice and data-driven governance. Its purpose is to establish a balance between the security imperatives of the criminal justice system and the fundamental right of citizens to know and to exercise public oversight. Grounded in the principles of transparency, accountability, and public participation, this concept seeks to enhance public trust in criminal justice institutions through improving the level of information dissemination. Within this framework, criminal management evolves from a purely reactive and punishment-oriented structure toward an intelligent, restorative, and protective system. In protective criminal management, non-confidential criminal information (such as crime statistics, institutional performance measures, and prevention indicators) is employed as an instrument of soft deterrence and social supervision. This approach, in addition to promoting transparency and efficiency, remains committed to safeguarding the privacy rights of victims and defendants. The present study, using an analytical–comparative method, examines the theoretical foundations of the "right to free access to information" and its impact on criminal justice in international instruments and in Iran's legal system. It further analyzes the existing structural deficiencies in the implementation of the Law on the Publication and Free Access to Information enacted in 2009. The findings indicate that achieving protective criminal management requires data integration among judicial and law-enforcement bodies, the formulation of judicial transparency regulations, and the institutionalization of a culture of accountability. Ultimately, such a model can provide an innovative framework for data-based, community-oriented criminal justice rooted in open governance within Iran's legal system.

Keywords: access obstruction; freedom of information; criminal management; cyberspace; criminal protection

1. Introduction

In the written and unwritten contract between the government and the people, one of the foundations of democracy is freedom of expression, free access to information, the dissemination of information, and the receipt of data related to political, administrative, judicial, and other public affairs by the people. The structure of power in a society based on respect for citizens' rights also recognizes these same rights for citizens in the domain of information dissemination. In Iran, the issue of publication of and free access to information, due to the existence of multiple interpretations and differing understandings regarding the manner of implementing this rule, was for a long time a subject of debate and disagreement, until the adoption of the law related to it in a given year finally, albeit belatedly, put an end to these disputes and ambiguities (Ansari, 2008).

Nevertheless, the vital importance of this law cannot be ignored, nor can it be overlooked that this law marks a transition from a stage of doubt and ambiguity to the opening of a new horizon of acknowledging the people's entitlement and their demands concerning news and information which, in contemporary life, are indispensable for participation in the governance of the country. The loss resulting from the absence of such participation is not borne only by the people and does not merely reinforce their lack of awareness; rather, it also inflicts damage on the government, the system, and public institutions. The higher the level of public awareness, the greater the possibility for responsible participation and prudent action by citizens in current affairs, and the more that critique, arising from new information and the presentation of innovative proposals for solving problems, can effectively contribute to the country's development.

Therefore, the existence of this law has brought us into a new environment in the fourth decade after the Revolution and directs public institutions toward providing information, publishing news, and informing the public, while at the same time guaranteeing the people's rights to free access to information and keeping them informed of the fine-grained issues and events—including those that may be fundamental in nature (Motamed Nezad & Motamed Nezad, 2007).

Such laws, in implementing the rights of the people arising from Principles 19 to 42 of the Constitution, can create a sense of security among individuals, because free access to information prepares the public to confront difficulties, to cooperate with the government in implementing programs, and to avoid rumor-mongering and the spread of unfounded reports across the country, as well as to refrain from relying on information obtained from unreliable channels. Unfortunately, this crucial matter had been neglected in previous years, and the market for rumors and recourse to foreign sources had become so heated that people obtained much of their news and information from other spaces. As a result, the discrepancy between information received from foreign sources and information published domestically led to a certain distrust and distancing from domestic media, particularly the national media, to the extent that it lost a significant portion of its audience.

This is while, in the view of experts, had such a law been implemented even a decade earlier, the likelihood of the occurrence of adverse political events—especially those witnessed in the late 2000s—would have been greatly reduced, or at least would not have reached such a damaging level. On this basis, and in light of the baseless political attacks and false accusations from Western actors and opponents of the system, centered on the alleged absence of democratic and popular structures in our country, it appears that the role of such laws in responding to these unfounded claims is a fundamental one and undoubtedly worth the costs that accompany it. However, what is considered crucial is not merely emphasizing freedom and guaranteeing the people's rights to obtain and freely access information; more important than that is determining the obligations and duties of public institutions to provide information whose disclosure is the people's right. This is because the people are the rights-holders, and the government and the three branches of power are the executors of the people's will and are obliged to meet their needs. On the basis of this law, in addition to guaranteeing these rights, the grounds for censorship and filtering of information must be reduced to a minimum. Of course, in cases where information relates to matters contrary to morality and the vital values of the country, specific legal standards still govern, and it is the duty of the government to shield the people from the harmful trajectory of such detrimental information and to protect them at the margins of security. However, institutions and agencies must not, under the pretext of preventing incorrect information, arbitrarily prohibit the provision and publication of information.

Creating the necessary structures and appropriate infrastructures for the implementation of this law is a prerequisite for practically adhering to the slogan "Knowing is the people's right." The first step in paving the way for enforcing this law is "culturalization and institutionalization." Our managers must believe in this law; our employees must consider themselves obliged to provide information to clients; and the people must be aware of what free access to information is and what rights are created for them under this law. Therefore, in order to create a public understanding of this law, profound cultural and educational work is required. If this law becomes established as a prevailing discourse and everyone speaks about it, it will naturally turn into a public demand.

On the other hand, the Law on Free Access to Information, to the same extent that it can have positive outcomes in preventing corruption, may also become a tool for defamation, character assassination, and a kind of political football; therefore, the cultural foundations for this law must be provided. The media, as one of the executive tools for this law, play an important and effective role both in generating public demand among the people and institutions, and in constructing a discourse around it. Naturally, having a free media environment and bringing news and media spaces closer to international standards is a precondition for implementing this law. Another requirement for enforcing this law is the availability of information in

electronic form and the realization of e-government. The best way to honor clients is the state's movement toward becoming electronic, which leads to the elimination of the complex path of administrative bureaucracy.

Although the main axis of implementing this law lies with the Ministry of Culture and Islamic Guidance, since the Ministry of Communications is supposed to provide the technical infrastructure for delivering information to the public, it is the most directly relevant ministry for enforcing this law. Moreover, the repeated emphasis by the Minister of Communications on implementing the Law on Free Access to Information, in itself, reflects the central role of this ministry in establishing a free flow of information (Ansari, 2008).

It appears that amending other laws in order to harmonize them with this law, and providing clear and precise definitions of concepts and red lines such as violation of sanctities, privacy, national interests and security, as well as integrating the archives of public and private organizations and making it possible for the National Archives to have access to all documents, are further measures that are necessary for the implementation of this law. Considering that the free flow of information, or freedom of information, in the early years of the twenty-first century has attained a special status and is referred to as the "oxygen of democracy," and that the implementation of this law in Iran can be regarded as a fundamental revolution in the administrative, executive, and macro-management system of the country, the present study seeks to examine the key mechanisms for free access to information.

2. Background

Rahimi (2013), in an article entitled "A Study of the Foundations of Free Access to Government Information and the Laws Related to It," states that freedom of expression is regarded as a fundamental right underlying all human freedoms and accesses; however, human needs require a constant rethinking of perspectives, and these perspectives themselves give rise to deep concepts such as "freedom of expression." Concepts such as "free access to government information" emerge from the approaches developed in line with freedom of expression which, although they may not appear similar to this principle at first glance, are in fact counted among its specific manifestations. In this article, an attempt has been made to present the history and background of the right of access, and the newly adopted law is likewise examined.

Besharati (2012), in an article entitled "The Role of Public Relations in Realizing the Principle of the Right to Free Access to Information in Democratic Systems," argues that what is certain is the direct connection between the right to free access to information and democracy, to the extent that in recent years free access to information has been described as the "oxygen of democracy." Therefore, before anything else, it is necessary to explain the intellectual foundations of democracy and the bases of democratic government in order to gain a general understanding of democratic regimes and, alongside this, to examine the right to free access to information in democratic societies. Subsequently, the article turns to defining public entities and explaining their main duties so that it becomes possible to make an accurate assessment of the claims that have been advanced.

Mohammad-Javad Rezaeizadeh and Yahya Ahmadi (2011), in their article on the foundations of citizens' right of access to governmental documents and information, emphasize that there are various reasons for the growing attention of states to the issue of citizens' right to access governmental documents and information. Among these are combating corruption, expanding citizen participation, improving the quality of public services, and enhancing individuals' standard of living through awareness of practical information. Other articles related to the subject of the right to free access to information also exist in this field. At present, people's free and unrestricted access to information is among the prerequisites for institutionalizing genuine democracy.

3. Theoretical Foundations:

3.1. Filtering

The concept of filtering or restricting information is much older and broader than the Internet. This concept can be traced back to "censorship." The Oxford English Dictionary (2014) defines censorship as "a mental power or force that suppresses specific elements in the unconscious and prevents them from appearing in the conscious mind. Censorship, as an official authority in some countries, is responsible for reviewing all books, periodicals, dramatic works, and the like before publication in order to ensure that they do not contain anything immoral, heretical, or offensive." In the literature, censorship has been

defined as the control of information and of the publication or circulation of ideas within a society. (Rabin, 2004; Zakeriyan, 2004) However, Internet censorship has not been properly defined and is undergoing a shift toward obfuscation, misuse, and propaganda. (Schneier, 2000)

The expansion of the Internet has created a situation in which a wide range of information can be disseminated across the world without any restrictions and beyond geographical borders, and the Internet has, in a striking way, been transformed into a communication and information medium. At the same time, the audience and users of the Internet have steadily increased. The nature and characteristics of the Internet, the ease of publishing material and information, and, in addition, the ease of accessing various types of information on the web—including text, audio, images, and diverse graphic data—have intensified to such an extent that, in some cases, information containing destructive and harmful content is also published on the web. This has paved the way for various forms of misuse. Pornographic content, particularly regarding the exploitation of children, the promotion of violence and corruption, the purchase and sale of harmful and addictive drugs, the dissemination of individuals' and organizations' private information, and the use of web-based information for terrorist purposes and similar cases have made it inevitable to control web content. Yet such control and supervision over the publication of information in different societies, depending on each society's political and cultural policies, has assumed different forms.

In some Western societies, the main emphasis is placed on preventing the misuse of individuals' private information, blocking the publication of sexual images of children, and preventing terrorist organizations from accessing specific and important information. By contrast, control of Internet content in Eastern and religious societies goes beyond these matters and includes strict supervision over the dissemination of political views and ideas on the global network. For example, in China—which ranks first in the world in terms of the number of Internet users—extensive monitoring of political information is carried out, and strict censorship is imposed on ideas and opinions that conflict with the Chinese communist government on the web. To this end, an "Internet police" has been established in that country. (Reno, 1999)

In another definition, Internet censorship or filtering is described as restricting the access of Internet users to websites and online services that, in the view of cultural and political authorities in each state, are not suitable for public consumption. The act of filtering is carried out by Internet service providers, but determining the levels, instances, and policies of filtering lies with governments. (Halder & Jaishankar, 2010)

3.2. Criminal Management

In an expanded and evolutionary perspective, criminal management is a multi-level and intelligent system that employs all components of criminal policy and criminal justice in a coordinated, data-driven, and ethics-oriented framework in order to balance crime control with social trust. This concept does not mean the traditional administration of judicial institutions alone; rather, it denotes a cross-sectoral and networked structure that organizes the interactions among the police, prosecution, courts, prisons, social institutions, and surveillance technologies. Its ultimate objective is to shift from a reactive and punitive criminal justice system to a preventive, reformative, and responsible one—a system that derives its legitimacy not from the severity of punishment but from the quality of public trust and institutional accountability. (Ebrahimi, 2011; Gholami, 2012)

Within this framework, criminal management seeks to elevate the criminal justice process from individual and fragmented decisions to systematic decisions based on the analysis of criminological data. Every stage of the criminal process—from social prevention to the execution of sentences—must, through data-based evaluation, be able to fulfill its role in safeguarding human security. Thus, the managerial philosophy of this system is not merely the control of criminal behavior, but the regulation of the relationship between the state, citizens, and collective trust within the framework of law. In this sense, criminal justice evolves from "penal authority" to "intelligent and accountable penal governance." In practice, modern criminal management rests on five interconnected pillars: (1) behavioral and environmental crime prevention through the analysis of social data; (2) investigation and detection based on an evidence-driven approach; (3) transparent and fair adjudication supported by judicial information technology; (4) targeted implementation of penalties focusing on the reform and reconstruction of the offender's personality; and (5) social reintegration and post-penal rehabilitation aimed at re-embedding the individual into society. These pillars are accompanied by performance evaluation systems and public reporting so that the structure of criminal justice

becomes a responsive, transparent, and ethics-based institution. (Hedayatvand & Others, 2012; Najafi Abrandabadi & Hashem Beigi, 1998)

Theoretically, the idea of criminal management is rooted in Garland's "culture of control" and in the teachings of Islamic criminal policy and Iranian penal rationality; both emphasize the need to replace a punishment-centered logic with a logic based on social trust and structural reform. (Gholami, 2012; Keenan, 2006) In fact, contemporary criminal management strives to link legal authority with social legitimacy so that criminal justice can be realized as a learning, feedback-sensitive system grounded in the analysis of human data. This transformation shapes a new face of justice whose aim is not merely punishment, but the creation of a knowledge-based and enduring trust system founded on ethics, law, and penal rationality. (Schonsheck, 1994)

3.3. Free Access to Information

Free access to information is one of the main foundations of transparent governance and communicative justice, by virtue of which every individual enjoys the right to be informed and to access the documents, data, and decisions of public institutions. In the Iranian legal system, this right has been recognized and guaranteed on the basis of the 2009 Law on Publication and Free Access to Information and in connection with Principles 24 and 175 of the Constitution, and is fundamentally grounded in the principle of the "right to know." According to this principle, citizens are not required to prove a personal interest in order to request public information, because information dissemination is a precondition for informed participation in the political, administrative, and justice-oriented life of society. In its essence, free access pursues two overarching objectives: first, to increase institutional transparency and accountability by making decisions and performance visible; and second, to prevent corruption, discrimination, and the abuse of power through public oversight. At the same time, freedom of information never means unregulated disclosure of data; it requires a delicate balance between the "right to know" on the one hand and "privacy, national security, and personal reputation" on the other. (Ansari, 2011a; Islamic Human Rights Commission of Iran, 2009)

In the field of criminal justice, this balance becomes doubly important, because free access can serve as a tool for monitoring the performance of judicial, law-enforcement, and investigative bodies, provided that the protection of procedural secrecy, the safeguarding of victims, and the security of the judicial process are not undermined. For this reason, the theory of "responsible transparency," discussed in contemporary freedom-of-information scholarship, is regarded as a practical framework for applying freedom-of-information principles in sensitive domains. From this perspective, freedom of information is not merely a media instrument, but a mechanism for consolidating trust between the state and society. Its proper implementation can strengthen the legitimacy of criminal justice, facilitate citizen participation in monitoring justice, and elevate justice from an administrative sphere to a social and communicative one, where knowing is considered part of the right to human dignity. Ultimately, achieving a "protective free-access" system requires structures for ethical oversight, education in information rights, and gradual policymaking for classifying data into public, semi-public, and confidential categories, so that the most institutionalized balance between transparency and security can be established. (Ansari, 2011b; Nobahar, 2008)

3.4. Criminal Protection

Criminal protection is a fundamental concept in criminal law and criminal policy that refers to the ensemble of legal instruments and penal mechanisms designed to safeguard the essential values of society—including life, dignity, freedom, property, public security, and social order. This concept signifies that criminal intervention by the state is justified only when other forms of protection (civil, administrative, or ethical) prove inadequate and when the violation of the protected values constitutes a serious threat to the public interest. Thus, criminal protection is not merely about punishing the offender, but about guaranteeing the most efficient and fairest form of social defense of the fundamental rights of individuals and the community.

From a theoretical perspective, the philosophy of criminal protection consists of three main dimensions: first, the axiological dimension, namely identifying the values and interests that merit protection in collective life; second, the instrumental dimension, that is, choosing penal means proportionate to the gravity and nature of the threat; and third, the normative dimension, meaning the determination of the boundaries of the legitimacy of criminal intervention so that individual freedom is not sacrificed to unrestrained surveillance. Consequently, criminal protection always has a dual aspect of protection and

limitation—protection of values accompanied by restraint on penal power to prevent encroachment upon citizens' rights. In the Iranian legal system, the concept of criminal protection is grounded in the principles of the Constitution (including Principles 19, 22, 23, 36, and 37) and has expanded through specific legislation, such as criminal protection of children and adolescents, women, the environment, personal data, and citizens' rights. This expansion reflects a shift from "retributive criminal protection" to preventive and supportive criminal protection based on dignity, rehabilitation, and social trust.

At the structural level, contemporary criminal protection no longer concerns only criminalization and punishment; rather, it covers the entire cycle of criminal policy—from identifying threats at the stage of prevention to fair trial and humane execution of sanctions. In this way, criminal protection forges an effective link with intelligent, data-driven criminal management, since criminal decision-making must be based on scientific risk assessment, proportionality of response, and evaluation of the social effects of each type of intervention.

3.5. Support-Oriented Criminal Protection of Free Access to Information

Differences in the accepted foundations of states' criminal policy lead to divergent approaches among the legal systems of various societies regarding recourse to penal sanctions within the framework of freedom-of-information regimes. This issue manifests itself clearly in the process of criminalization.

In liberal and libertarian systems, citizens' rights—such as the right to information—are given such a high level of normative weight that, out of fear of infringing these rights through restrictive criminalization, policymakers proceed with extreme caution and, in principle, adopt a strategy of avoidance. However, such a libertarian approach can no longer be observed in any society today, at least not in the field of freedom of information. In reality, governments usually approach the issue with authoritarian, security-oriented, or moralizing attitudes, or with a combination of these. (Nobahar, 2008)

In authoritarian systems, state sovereignty and governmental interests are considered so important that citizens' right of access to information—which is essentially regarded as a constraint on the freedom of action of officials—is recognized only within the framework of preserving state power. In an authoritarian approach, the recognition of any institution or entity whose existence requires action independent of state authority is not accepted, though such independence is intrinsic to a freedom-of-information regime. This situation can be observed in some countries, such as Saudi Arabia, which has even refrained from clothing the freedom-of-information institution with the apparel of law and, conversely, readily resorts to penal sanctions to restrict the provision of information to persons outside the ruling structure. For example, Article 5 of that country's Law on the Punishment of the Disclosure of Confidential Documents and Information, enacted in 1432 AH (2011 CE), prescribes for mere commencement of the offense of disclosing or providing information a maximum penalty of ten years' imprisonment and a fine of one million riyals.

In security-oriented systems, by emphasizing concepts such as safeguarding security and maintaining public order, efforts are made to establish a narrow and restrictive framework for implementing the freedom-of-information regime. Security-orientation does not necessarily go hand in hand with authoritarianism; non-authoritarian regimes may, under specific circumstances, also adopt a security-oriented stance and, when confronted with a conflict between "freedom" and "security," give priority to the latter. Such a preference may sometimes serve merely as a pretext for sacrificing freedom and social rights, or it may, in certain conditions, genuinely compel the government to restrict freedoms, including freedom of information. In a purely authoritarian perspective, what matters is the security of the state and government itself, not the security of society as a whole and in a way that encompasses the security of individual citizens.

In ethics-oriented systems, by focusing on a kind of moralism, restrictions on freedom of information are imposed through appeal to moral concepts and criteria, treating anti-moral notions—such as affronts to public decency or violations of privacy—as standards for limiting freedom-of-information regimes. Despite the differences in the substance of these three approaches, it must be said that excessive inclination toward any of them may manifest itself in a reduction of positive criminal protections and an increase in negative criminal protections, that is, protections that in practice restrict access to information. Some states' enacted laws attest to this fact.

For example, Turkey's Law on the Right to Information—despite including Article 29 under the heading of penal provisions—under no circumstances authorizes the implementation of penal sanctions for non-compliance with freedom-of-information rules and refrains from providing for positive criminal protections. It explicitly stipulates that, "without any

insistence on prosecuting violators under the general rules of criminal law, officials and public employees who, out of negligence, carelessness, or deliberate intent, prevent the implementation of the provisions of this law shall be subject to disciplinary sanctions applicable to the administrative staff." Meanwhile, in that same country's criminal justice system, by adopting the same threefold approaches, efforts have been made to expand negative criminal protections that, in practice, limit access to information. Articles 239, 258, 326, 327, 331, and 333 of the 2004 Penal Code bear witness to this, as they envisage multiple life sentences in this field and even prescribe up to eight years' imprisonment for the mere possession of confidential information.

In reality, instead of excessive criminal interventions that imply positive protection of freedom of information on the one hand, and neglectful criminal interventions that imply negative protection of that regime on the other—interventions influenced either by prioritizing the right to information over other rights such as the right to security, the right to privacy, and moral considerations, or by marginalizing freedom of information in favor of those other rights—the architecture of a system of criminal information law can and must be shaped through the establishment of balance and equilibrium among these reconcilable rights. Any neglect or deliberate disregard of either side will disturb the two-way relationship between rulers and the ruled and lead to widespread dissatisfaction.

Within this legal framework, a particularly influential right in determining the course of criminal information policy is the right not to be punished. In Islamic criminal law, this right is expressed in principles such as the presumption of innocence and the principle of permissibility. The implication of this right—which establishes the primary rule of criminal law on the basis of non-intervention—is that its violation, which occurs via the mechanism of criminalization, is justifiable only by reference to several principles and within certain limits. (Khosroshahi & Danesh Pajooh, 2000)

In Islamic criminal law, except for a limited number of offenses that are subject to ḥadd or qiṣāṣ punishments and have been directly criminalized by the sacred Lawgiver, the remaining offenses—constituting a large portion of the catalogue of crimes—fall under the taʿzīr system, which is left to the discretion of the ruler. Criminalization in the domain of freedom of information is likewise to be analyzed within this sphere. In line with what has been mentioned, the governing criminal system must refrain from entering the realm of freedom of information—just as in other domains—unless criminalization principles dictate otherwise.

In this context, the view of a criminal-law philosopher named Jonathan Schonsheck contains noteworthy ideas. He believes that "when we seek to criminalize a given behavior, that behavior must successfully pass, in a sustained and effective manner, through three distinct filters. If it fails to pass through these filters, it cannot be considered a crime; only if it passes all three can the criminalization of the conduct be justified." Schonsheck's innovation of the "filtering-in-the-process method" rests precisely on this premise. (Schonsheck, 1994)

4. Free Access to Information under the Shadow of Filtering

4.1. The Principle Filter

On the basis of this filter, it must first be established that, according to the theoretical principles of criminalization, the conduct in question falls within the jurisdiction of the community's judicial authority or the sphere of state power. In other words, it must be demonstrated that, from the standpoint of theoretical principles and foundations, the state is permitted to intervene in the realm of citizens' individual rights and freedoms through prohibition or the imposition of criminal restrictions.

In this regard, two main principles can be invoked:

a. The Harm Principle.

The most important guiding principle in the field of criminalization in most criminal justice systems is the harm principle. In the liberal approach, "harm to other citizens" is presented as the paradigm of harm. John Stuart Mill, in this context, has stated that "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others" (Keenan, 2006).

There is disagreement among jurists about the definition of harm. Feinberg's analysis in this regard has gained widespread acceptance among Western thinkers. He maintains that "criminalizing an act is justifiable only where it is effective in preventing harm to others, or reducing its extent, or in preventing the creation of severe offense for others." Clarkson, a distinguished

English jurist, while accepting this definition, considers harm to mean "neutralizing, pushing back, or depriving a person of a benefit" as the result of another's wrongful conduct.

On the basis of this understanding, positive criminal protections for the freedom-of-information regime must be confined to refraining from withholding only such categories of information whose non-disclosure will cause direct harm to citizens, or, in light of the broader concept mentioned, will deprive them of acquiring a benefit. From Articles 7 and 22 of the Law on Publication and Free Access to Information, it may be inferred that the criminal-law approach of our legislator has not centred the axis of criminalization in the field of freedom of information on the harm or deprivation of the benefit of the requester, even though in some cases non-disclosure of information may indeed produce such a result.

With respect to negative criminal protections for freedom of information, the harm principle is generally observed in determining sanctions for accessing those categories of information that fall under harm-based exceptions. Hence, the criminalization of access to information that harms interests such as the health of others or the trade secrets of third parties can be justified in this direction. For example, Principle 15 of the Johannesburg Principles, under the heading "general rule on the disclosure of classified information," expressly provides that "no one may be punished for disclosure of information on grounds of national security if the disclosure does not pose real and demonstrable harm to a legitimate national security interest, or if the public interest in knowing the information outweighs the harm caused by its disclosure."

Regarding information that falls under category-based exceptions—such as state secrets—or even certain types of information falling under harm-based exceptions—such as information prejudicial to security, information related to tax assessment and collection of lawful dues, or information concerning immigration control—where no specific individuals necessarily suffer direct harm, this principle will not be sufficient. In such cases, it is society as a whole that suffers injury. For that reason, some who define harm in the narrow sense mentioned have recourse to a complementary principle, the welfare principle, to justify the criminalization of these latter types of conduct. This principle authorizes the criminal justice system to criminalize behaviours that disturb public peace and order.

In Islamic criminal policy, harm is understood in a broader sense than harm to specific individuals; it also encompasses harm to religion, to society, and even to the offender himself (Khosroshahi & Danesh Pajooh, 2000). Therefore, it becomes unnecessary to resort to additional principles such as the welfare principle. There is ample evidence in support of this view; for example, some religious texts explicitly refer, regarding certain offenses, to the rationale of "harm to religion, society, and the self" in the prohibition of particular acts or in the proscription of engaging in them.

b. The Principle of Censure.

According to this principle, a conduct can be characterized as a crime only if, from the standpoint of social judgment, it is blameworthy and deserving of condemnation. How such blameworthiness is determined has been explained thus: when an act crosses the threshold of moral tolerability, it must be criminalized. The inseparable connection between this principle and a society's moral values has led some authors to refer to it under the heading of "legal moralism," which has been sharply opposed by the liberal school.

It appears that, in Islamic criminal policy, alongside the harm principle—which entails the prohibition of inflicting harm—the offender's blameworthiness has also been considered necessary for criminalizing conduct. On the basis of this mode of thinking, in cases where a person's act harms others but he has been authorized to perform that act—such as digging a well on one's own property—no liability will be established if others are harmed.

In light of the jurisprudential foundations of freedom of information previously discussed, since information held by governmental institutions has the character of a trust (amānah), both the failure to disclose such information to the people where there is no legitimate impediment, and its disclosure in prohibited circumstances, amount to breach of trust. Because this behaviour violates an ethical and fiduciary commitment, punishing the perpetrator is justified. The anti-moral character of the conduct is even more pronounced where the information relates to individuals' privacy, constitutes an instance of disseminating obscenity, or has come into the institution's possession by virtue of a relationship of confidence.

In this same vein, it can be observed that in some countries, despite the fact that their freedom-of-information laws do not provide negative criminal protection with respect to information that harms governmental interests, they have nevertheless resorted to criminalization with regard to information that violates privacy or infringes the right to health of others.

At the end of this section, it is possible to point to certain problems in the scope of criminal interventions in the field of freedom of information that do not conform to the principles of criminalization. For example, the legislator, in paragraph (b)

of Article 22 of the Law on Publication and Free Access to Information, has considered obstruction of the performance of the duties of the Commission on Publication and Free Access to Information to be punishable. In light of what has previously been stated regarding the legal function of this Commission, it becomes clear that, unlike similar bodies in other legal systems, this Commission does not play a significant role in the field of freedom of information. Therefore, such criminalization neither serves the purpose of criminal prevention of any substantial harm, nor does it carry an anti-moral quality that would warrant censure. On this basis, it is difficult to justify the legislator's recourse to criminalization in this regard.

4.2. The Presumptions Filter

Once a given conduct has passed through the filter of principles, criminalization cannot be justified without examining whether there exist other, more appropriate methods of preventing the behaviour outside the framework of the criminal justice system. The presumptions filter states that methods which create the least interference for the individual and have the weakest coercive dimension are preferable to methods that impose greater inconvenience and constraint. Accordingly, in the realm of freedom of information as well, recourse to criminal protections should only be made where no other protective mechanism is available.

With regard to the basic legitimacy of employing criminal sanctions to safeguard freedom of information, there is no particular difficulty: in this system, public officials—who, by virtue of their superior position, are deemed to be under specific duties—are not reasonably expected to be bound merely by informal reactions or even formal but non-criminal measures, the enforcement of which is not seriously guaranteed. Nevertheless, with respect to the temporal stage of resorting to such criminal measures, greater hesitation and deliberation are required.

One of the problems observable in the statutory rules of information criminal law—as reflected in Article 22 of the Law on Publication and Free Access to Information and in the provisions that establish negative protections—is that the legislator has immediately resorted to the criminal-law weapon. It would appear that if the legislator had initially made use of other tools, such as administrative-disciplinary sanctions, and only in cases of repetition proceeded to criminalize the conduct, more favourable effects in securing the free flow of information could have been achieved. In that event, judges might also have shown greater willingness to impose sanctions on offenders, and this, in turn, would have prevented the rules on criminal protection of freedom of information from becoming practically obsolete and inoperative—"dead letters," so to speak. Yet this is precisely what is not perceived in the enforcement record of criminal protections for freedom of information in our country. One member of the Guardian Council, who is active in the field of media law, stated at a conference in 2009:

"In the amendments made to the Press Law in 2000, we can see attention to this right of access. Unfortunately, however, judicial practice has not been able to help us derive much benefit from this legal institution… In fact, this right already existed in the Press Law of 1985. Yet I, as someone interested in these issues who follows court practice in this domain, have not encountered a single case in which a judgment has been issued—and effectively enforced—against an official for obstructing journalists' right of access to information."

He goes on to note that, in the 2000 amendments to the Press Law, a note was added providing that the offender, if there is a complainant, shall be sentenced by the court to dismissal from public service for a period of six months to two years, and, in case of repetition, to permanent dismissal from government service; and yet, despite the existence of this note, he is unaware of any judgment that has been issued under it (Ismaili, 2007).

In some countries, the temporal deferral of criminal punishment in dealing with violations of freedom-of-information rules has been regulated in an appropriate manner. For example, in Mongolia, Article 25 of the Law on Information Transparency and the Right to Information provides that, on first commission, the violation by a public official is subject only to disciplinary–administrative sanctions, and, in cases of repetition or serious gravity of the act, dismissal from public service is ordered by the competent administrative authority. The interesting point here is that, in the event that the relevant authority refuses to impose the prescribed disciplinary sanction, in order to secure compliance with the criminal provisions, a monetary fine equal to five times the minimum salary of that authority is stipulated.

4.3. The Functions Filter

After a conduct has passed through the previous filters, it must undergo a third stage of screening, in which the practical consequences of its criminalization are examined. The enactment and implementation of criminal laws always entail social consequences: some of these effects are obvious and manifest quickly, while others may take a long time to appear and may be quite unexpected or surprising. In reality, the social costs and benefits of enforcing or not enforcing the proposed criminal law must be evaluated and weighed.

In the context of criminalization in the domain of freedom of information, given that such violations are typically committed by public officials and agents of the state, the legislator—by enacting criminal provisions and prescribing penalties for such conduct, and, alongside this, providing adequate public and administrative awareness about the criminal consequences of depriving individuals of lawful access to information—effectively realizes the expressive and descriptive function of criminal law in protecting social values. At the enforcement stage, by obliging state employees to fulfil their duties, the legislator thereby facilitates the realization of citizens' right to information.

However, a subtle point that must not be overlooked here concerns criminalizations adopted in the name of negative protection of freedom of information. Excessive resort to such criminalization can lead to an overcautious attitude among public officials in providing information to the public, out of fear that their conduct might fall under some criminal heading. The gradual effect of such a situation is that information will not be transmitted to society, a culture of secrecy and confidentiality will dominate the government, and the ground for corruption will be prepared.

For this reason, in some recommendations issued by international human rights bodies, it is emphasized that individuals should be protected against any legal, administrative, or employment sanctions for disclosing information related to violations such as criminal activity or fraud, failure to comply with legal obligations, miscarriage of justice, corruption or deceit, or serious mismanagement in public institutions. In a growing number of countries that recognize the importance of public access to government-held information, journalists and other media actors incur no criminal liability in relation to government information—even if classified—so long as disclosure does not pose a risk of serious harm to national security and, in some jurisdictions, to international relations. For example, courts in England, where disclosure has been in the public interest, have refrained from imposing punishment even in the presence of a binding duty of confidentiality.

In our own legal system, Article 4 of the Press Law, in order to ensure protection of the press, provides that "no governmental or non-governmental authority has the right to exert pressure on the press for printing any item or article, or to resort to censorship or control of publications." Note 1 to Article 5 stipulates, for those who violate this rule, dismissal from public service for a period of six months to two years and, in case of repetition, permanent dismissal. This provision can have a highly significant impact on the criminal protection of society's right to information, through safeguarding the institutional position of the media.

Moreover, in the cultural policies of the Islamic Republic of Iran in the field of the press, adopted by the Supreme Council of the Cultural Revolution in 2001, it is expressly provided—so as to prevent unjust criminal prosecution of media professionals for performing their informational duties, which may involve criticism of governmental bodies—that:

"Within press cultural policy, scientific criticism, logical debate, raising questions on religious issues, and criticism and review of government performance, so long as they do not undermine religious beliefs, impair adherence to Islamic rules, or infringe public rights, do not fall under the heading of 'subversion' (ikhlāl). Subversion is not an intentional offense per se; where lack of mens rea—that is, absence of criminal intent—is established, this shall be considered in mitigation or pardon."

The same resolution explicitly states that "accurate, timely, and honest information aimed at reflecting views, constructive criticisms, suggestions and explanations by the people and officials, as well as raising problems and pointing out shortcomings with the aim of diagnosing root causes and gaining a more precise understanding of issues in order to find appropriate and constructive solutions for the country's progress, with due regard to Islamic norms, the interests of society, and the Constitution," does not fall under the concept of subversion.

Principle 16 of the Johannesburg Principles likewise provides, concerning disclosure of information by public officials, that "no person may be subjected to any detriment or sanction, on grounds of national security, for disclosing information that he or she has obtained by virtue of public employment, provided that the public interest in knowing the information outweighs the harm resulting from its disclosure."

One of the reasons why the Iranian legislator, in the Law on Publication and Free Access to Information, has refrained from establishing negative criminal protections appears to be precisely the concern that criminalization in this sphere may increase the risk that society will be deprived of access to information.

In addition, since officials who disclose information in their possession may subsequently be subjected to retaliation by superior authorities, it is necessary—beyond granting them immunity from any judicial or administrative prosecution—that, so long as their bad faith has not been established, they receive the necessary protection if they are harmed; and that those who retaliate against them face effective deterrent sanctions.

In any event, it is incumbent upon the legislator to frame sanctions for safeguarding the freedom-of-information regime in the same manner as in other criminal domains: they must be neither so lenient that individuals feel no fear in committing violations, nor so harsh that courts are reluctant to impose them. From a procedural standpoint as well, such cases must be heard out of turn and without excessive formalities, so that citizens are not discouraged from seeking the protection of the law and the deterrent force of the sanctions is preserved.

5. Conclusion

The expansion of the Internet created a space in which a wide range of information could be disseminated across the globe without any effective limitation. At the same time, the spectrum of internet users was as broad and diverse as its content. Unlimited access to information, and the fact that anyone could access any kind of material, caused anxiety for many and provoked sharp criticism. One group of critics consisted of those who objected to immoral and unethical online content, viewing it as harmful and corrupting, particularly for young people and adolescents. The other group was made up of governments that could not tolerate dissenting voices. For years, these governments had sought to impose their own ideology and worldview on their populations by keeping society closed and controlled, and by censoring traditional media such as the press and newspapers, and in doing so, they confronted any form of modernity or intellectual dissent that conflicted with their preferences. It is therefore unsurprising that such regimes perceived the Internet and the uncontrolled circulation of information as a serious threat to their very existence and moved to combat it. Since most of these governments have simultaneously tried—contrary to their true nature—to present a democratic and freedom-loving image of themselves, they could not openly admit the real reason for their opposition to the free flow of information. Thus, they joined the first group and raised the banner of combatting corruption and immoral content.

In any case, neither of these two groups could truly escape the Internet. The scientific and cultural achievements associated with the Internet were so remarkable that ignoring them was hardly possible. Given that the Internet is a global network and, by virtue of its architecture, no group or state can exercise full control over the content disseminated through it, the idea gradually emerged that instead of controlling the production and publication of content, control should be exercised over users' access to and use of the Internet.

It was at this point that the term "filtering" entered the vocabulary of the online world. In ordinary language, filtering means purification and the removal of impurities; in the context of the Internet, it refers to preventing users from accessing websites that contain inappropriate content—although the definition of "inappropriate" itself is highly contested.

At present, a large portion of online content relates to religious matters. What officials initially feared has, in many respects, materialized, and it is to be expected that they have resorted—even by non-humanitarian and unethical means—to counter it. Information dissemination has reached a level where any user can upload and share materials on this global information network that may be anti-religious or anti-ethical. Not only our country, but other states such as the United States, China, and Russia have also taken measures—under the heading of filtering—to prevent online attacks against their political, ethical, and other perceived national interests. The capitalist United States shows particular sensitivity toward criticisms directed at this economic system, and much of what is filtered in that country consists of content that criticizes or rejects capitalism. In Saudi Arabia, where women still lack a proper status in the social affairs of the country, any content concerning women's right to vote, their freedom to participate in social life, or even their right to drive is subject to filtering.

The Islamic Republic of Iran, which has long been the target of various forms of cultural aggression and "cultural invasion," adopted a law in 2001 on filtering immoral websites. Following this, any content that exhibits open hostility and antagonism toward Islam and the Shi'a school has been classified among the targets of filtering. The laws and rules of the Islamic Republic

of Iran are derived from the authentic principles of the noble religion of Islam and are based on the Book of God (the Qur'an) and the Sunnah of the Holy Prophet of Islam, as well as the teachings of the Infallible Imams (peace be upon them). Accordingly, by referring to firm jurisprudential proofs, certain cases have been identified as manifest violations of the Sharia, and the state has moved to prevent their dissemination on the national internet.

In Islamic jurisprudence, what has been used as the principal doctrinal basis for this kind of filtering is the notion of "deviant (misguiding) books," whose purchase, sale, possession, and dissemination have been declared prohibited in light of the purport of certain Qur'anic verses and the meaning of relevant narrations. Although some objections and doubts have been raised regarding the soundness of these proofs and it has been argued that their evidentiary value for the desired conclusion is not complete, nonetheless, no scholar has gone so far as to deem such activities permissible.

Another argument sometimes raised concerns the intellectual and rational maturity of contemporary society and the claim that, given people's deeper insight today compared to the past, such books can no longer undermine their beliefs. This argument is also not widely accepted, for even assuming a higher level of rational development, failure to prevent content that leads to insult, denigration, or weakening of religion and the madhhab cannot be considered permissible; certain forms of opposition that clearly stem from malice and hostility are never acceptable to disseminate under any circumstances. Yet another claim is that making such materials available increases people's insight and awareness, enabling them to distinguish truth from falsehood more clearly, and that such discernment ultimately strengthens the religious foundations of society.

Taken together, however, the overall conclusion is as follows: content that is subject to filtering and blocking in our country is restricted on the basis of the jurisprudential foundations of Islam, and the provisions contained in the Constitution and in the Islamic legal framework of the state are drawn from Islamic teachings. Currently, approximately fifty categories have been identified and codified in law; if a website or weblog violates even one of these categories or serves as a means for activities that fall within their scope, the national filtering authority is legally entitled to suspend or block that site or weblog.

6. Suggestions

1. On the Internet, as in other media, the principle of minimal state intervention should be upheld. Policymaking and the implementation of filtering should be entrusted to independent bodies, and governments should assume the role of advisor and supporter of these institutions, rather than direct controller.
2. A specific filtering page should be designed and displayed for addresses that are blocked without direct human review (for example, those identified by automated robots or appearing on pre-compiled blacklists).
3. A distinct filtering page should be provided for addresses whose content is genuinely unethical or pornographic, clearly explaining the grounds for blocking in terms understandable to users.
4. Filtering should be made more targeted and purposeful, and efforts should be made to prevent its excessive expansion, overblocking, and the unjustified inclusion of lawful and useful content within the scope of restrictions.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

References

Ansari, B. (2008). *Freedom of Information*. Dadgostar Publications. https://tp4.ir/academy/

Ansari, B. (2011a). A Comparative Study of the Right to Access Media to Judicial Proceedings and Legal Information. *Legal Research*, *35*. https://www.gisoom.com/book/11300342/

Ansari, B. (2011b). *Rights of Private Domain*. Organization for Human Sciences Research and Book Writing of Universities: Samt. https://fa.wikifeqh.ir/

Ebrahimi, S. (2011). *Criminal Identification and Prevention* (Vol. 1). Mizan Publications. https://www.hovalvakil.com/product/1922

Gholami, A. (2012). *From Good Morality to Ethical Security: A Study in the Criminal Policy of the Islamic Republic of Iran and Imamiyah Jurisprudence*. Imam Sadiq University Publications. https://www.gisoom.com/book/1847832/

Halder, D., & Jaishankar, K. (2010). *Cyber Crime and Victimization of Women: Laws, Rights, and Regulations*. LGL Global. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1561774

Hedayatvand, M., & Others. (2012). *Decision-Making Procedures in Administrative Law: A Comparative Study*. Kharsandi Publications. https://ketabrah.com/search?q=

Islamic Human Rights Commission of Iran. (2009). *Human Rights in the Contemporary World: Concerns and Perspectives of Iranian Jurists and Scholars*. Ahmadi Publications. https://www.gisoom.com/book/1636342

Ismaili, M. (2007). Freedom of Communications and Information in Islamic Law and Teachings. *Media Journal*, *69*. https://mohsenesmaeili.ir/?p=601

Keenan, P. J. (2006). The New Deterrence: Crime and Policy in the Age of Globalization. *Iowa Law Review*, *91*. http://ssrn.com/abstract

Khosroshahi, Q., & Danesh Pajooh, M. (2000). *Philosophy of Rights*. Imam Khomeini Educational and Research Institute. https://www.gisoom.com/book/1763743/

Motamed Nezad, K., & Motamed Nezad, R. (2007). *Communications Rights*. Office for Media Studies and Development. https://agahbookshop.com

Najafi Abrandabadi, A. H., & Hashem Beigi, H. (1998). *Criminal Identification Encyclopedia*. Shahid Beheshti University Publications and Knowledge Ganj Library. https://ganjedanesh.com/fa/product/50688

Nobahar, R. (2008). *Support for Criminal Rights from Public and Private Spheres*. Jungle Javadaneh Publications. https://www.gisoom.com/book/1509477/

Rabin, R. (2004). *Foundations of Bibliography and Information Science*. Rayaneh Book Publications. https://www.gisoom.com/book/1499089/

Reno, J. (1999). Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry. http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Schneier, B. (2000). Semantic network attacks. *Communications of the Acm*, *43*(12), 168. https://dl.acm.org/doi/pdf/10.1145/355112.355131

Schonsheck, J. (1994). *On Criminalization; An Essay in the Philosophy of the Criminal Law*. Kluwer Academic Publisher. https://doi.org/10.1007/978-94-015-8100-4

Zakeriyan, M. (2004). *Key Concepts of Human Rights in the International Arena*. Mizan Publications. https://mizan-law.ir/Book/Details/363