Research on Personal Information Protection Mechanism from the Perspective of Information Disclosure by Administrative Authorities

Tianyi Guan
School of Law, Xinjiang University of Finance and Economics, Urumqi, Xinjiang, China

Abstract: Driven by the dual needs of digital governance and rights protection, the value conflicts between information disclosure by administrative authorities and personal information protection have become increasingly prominent. While information disclosure by administrative authorities centers on safeguarding citizens' right to know and improving administrative transparency, personal information protection aims to uphold personal rights and information security. The two present a complex relationship of intersection and game in administrative practice. At present, problems such as ambiguous definition of personal information, absence of review procedures, lack of de-identification mechanisms, and inadequate relief channels exist in the information disclosure of administrative authorities, which seriously infringe upon citizens' personal information rights and interests. From the perspective of administrative law, this paper systematically analyzes the logic of value balance between information disclosure by administrative authorities and personal information protection, sorts out the current legal norms and practical dilemmas, and combines typical cases to construct a personal information protection mechanism featuring legitimacy, security and effectiveness from four dimensions: definition criteria, review procedures, technical de-identification and relief mechanisms. It provides theoretical support and approaches for institutional improvement to achieve a dynamic balance between the protection of the right to know and personal information rights and interests.

Keywords: Information Disclosure by Administrative Authorities; Personal Information Protection; The Right to Know; Administrative Review; Administrative Remedy

1. Introduction

In the context of digital government, administrative agencies have become key entities in the processing of personal information [1]. Government information disclosure is a hallmark institution of a modern government governed by the rule of law. The Regulations of the People's Republic of China on the Disclosure of Government Information establish the basic principle that "disclosure is the norm, and non-disclosure is the exception," serving as a core norm for safeguarding citizens' right to know and for overseeing administrative power. With the enactment of the Personal Information Protection Law of the People's Republic of China, personal information has been separated from the traditional scope of privacy rights, forming a specialized and systematic framework for rights protection that clarifies the specific obligations and responsibilities of state organs in processing personal information. Within the tiered protection system for personal information, the Personal Information Protection Law and related laws and regulations provide the strictest protection for sensitive personal information [2].

In the course of performing their administrative functions, government agencies collect, store, and generate vast amounts of personal information containing details such as individuals' identities, property, health, and whereabouts. Such information possesses dual attributes as both "government information" and "personal information," placing it at the intersection of the government information disclosure and personal information protection systems. In practice, the conflict of values between these two areas continues to intensify: on the one hand, to implement the requirement of "disclosing as much as possible," grassroots administrative agencies often fail to de-identify sensitive information when making public disclosures, resulting in the "exposure" of

personal information and turning it into a source for telecommunications fraud and doxxing. Data breaches and privacy violations are becoming increasingly frequent, placing higher demands on the protection of privacy rights and personal information within the context of government information disclosure [3]. On the other hand, some administrative agencies, citing "the protection of personal privacy," abuse their discretionary power to withhold information, arbitrarily expanding the scope of exemptions and refusing to disclose government information involving the public interest. This undermines the system safeguarding the right to know, creating a practical dilemma where "letting go leads to chaos, while strict control stifles progress."

2. Conflicts and Balances between Government Information Disclosure and Personal Information Protection

2.1 The Opposition and Unity of Core Values

The right to know serves as the legal foundation for government information disclosure. Its core essence is that citizens have the right to access information regarding administrative agencies' performance of duties, decision-making processes, and public affairs. This right aims to break the monopoly on administrative information, ensure public participation, and oversee the proper exercise of administrative power. The right to personal information is a personal right established by the Personal Information Protection Law. Centered on safeguarding the tranquility of natural persons' private lives, information autonomy, and information security, it encompasses specific elements such as the right to determine information, the right to know, the right to use, and the right to seek remedies. Disagreements persist regarding the inherent attributes of personal information and the definition of personal information rights, leading to disputes over the attribution of interests related to personal information and, consequently, giving rise to conflicts of interest [4]. The relationship between government information disclosure and the protection of personal privacy is, in essence, a balance between public interest and individual interest [5].

There is a clear conflict of values between the two: the right to know emphasizes the "openness" of information, requiring administrative agencies to disclose public information to the greatest extent possible to safeguard the public's rights to oversight and participation; the right to personal information emphasizes the "confidentiality" of information, requiring restrictions on the arbitrary collection, disclosure, and misuse of personal information to uphold the dignity and private interests of natural persons. This opposition is essentially a balancing act between public and private interests. If too much emphasis is placed on government information disclosure, it may lead to the illegal leakage or misuse of personal information, thereby infringing upon citizens' private rights; conversely, if too much emphasis is placed on personal information protection, it may lead to administrative agencies abusing exemption clauses to evade their obligations of information disclosure, thereby hindering the realization of the right to know.

The two share an intrinsic unity: both aim fundamentally to safeguard citizens' rights and regulate the exercise of public power. Legitimate government information disclosure is a prerequisite for personal information protection; only by clearly defining the scope and procedures for information disclosure can we prevent administrative agencies from evading their disclosure obligations under the pretext of "protecting personal information"; Comprehensive personal information protection serves as the baseline for government information disclosure. Only by fortifying the institutional defenses of personal information protection can government information disclosure proceed in an orderly manner within the framework of the rule of law, thereby preventing "unprotected disclosure" from harming citizens' rights. The two are mutually reinforcing and dialectically unified, jointly serving the core values of administrative rule of law and the protection of citizens' rights, and achieving a dynamic balance between public and private interests. Information, with its content as the object of legal relations, is processed by the human mind, and its corresponding subjects are traditional social entities such as natural persons and legal entities; data, with its form as the object of legal relations, is processed by computer systems, and its corresponding subjects are new types of social entities such as online platforms and artificial intelligence organizations [6].

2.2 The Core Essence of the Principle of Balance

Achieving a dynamic balance between the two requires adherence to five core principles, which provide clear guidance for administrative disclosure practices and judicial review: First, the principle of legality and legitimacy, whereby disclosure must have a legal basis and comply with statutory procedures; second, the principle of minimal necessity, limiting the scope of disclosure to the minimum required to fulfill the right to know, with priority given to de-identification; third, the principle of differentiated treatment, requiring the removal of sensitive content from mixed information and prohibiting a "one-size-fits-all" approach; fourth, the principle of public interest priority, whereby personal information protection yields to significant public interests while adhering to the principle of proportionality; and fifth, the principle of security assurance, requiring administrative agencies to fulfill their obligations for end-to-end security management of disclosed information. Theoretically, applying the principle of proportionality—as a balancing method—to the review of administrative agencies' personal information processing activities is the "only way" to achieve the dual objectives of the reasonable utilization of personal information and the protection of individual rights [7].

3. Practical Issues in Personal Information Protection within Government Information Disclosure

3.1 Confusion Regarding the Criteria for Defining Personal Information and Privacy

Ambiguous conceptual definitions constitute the primary issue in personal information protection within current government information disclosure. This is primarily manifested in inconsistent criteria for distinguishing between personal information and personal privacy, a lack of identification of sensitive personal information, and an overly broad definition of public interest. Consequently, administrative agencies face difficulties in accurately determining the boundary between disclosure and protection in practice.

First, the scope is not clearly defined. The "Regulations on the Disclosure of Government Information" uses the term "personal privacy," while the "Personal Information Protection Law" employs the concept of "personal information." Although there are differences in the connotations and denotations of these two terms, current regulations do not specify the criteria for their integration within the context of government information disclosure, causing administrative agencies to confuse the boundaries between them in practice. Second, there is a lack of identification of sensitive information. Current regulations have not established a unified classification system for sensitive personal information, and administrative agencies lack clear guidance on identifying such information, making it difficult to accurately distinguish between general personal information and sensitive personal information. No special protection rules have been established for high-risk sensitive information, leading to the arbitrary disclosure of such information and posing serious security risks. Third, the definition of public interest is overly broad. Some administrative agencies abuse the "public interest" exception clause, arbitrarily expanding the scope of its application under the pretext of "supervisory needs" or "public disclosure requirements," thereby disclosing personal information that should otherwise be protected.

3.2 Prior Review and Procedural Safeguards Are Merely a Formality

The review mechanism is a core component of personal information protection in government information disclosure. However, the current information disclosure review mechanisms in China's administrative agencies suffer from issues such as unclear responsibilities, procedural gaps, and inadequate differentiation in handling, resulting in prior reviews becoming a mere formality and making it difficult to effectively prevent the risk of personal information leaks.

First, the reviewing authority is unclear. Most administrative agencies have not established dedicated review bodies for information disclosure and personal information protection; instead, the review of information disclosure is handled by the relevant functional departments themselves. Reviewers lack professional legal knowledge and awareness of personal information protection, making it difficult for them to accurately identify personal and sensitive information, and they are unable to conduct reviews in strict accordance with

statutory procedures, resulting in a lack of independence and professionalism in the review process. Second, review procedures are lacking. Administrative agencies have failed to strictly enforce the written third-party consultation procedure stipulated in Article 32 of the Regulations on the Disclosure of Government Information. When disclosing government information containing personal information, they often decide to disclose it directly without consulting the rights holders, thereby disregarding the rights holders' right to determine the disclosure of their information. Third, inadequate differentiation and handling. For government information that mixes personal information with public information, administrative agencies have failed to adequately distinguish and process the two, often disclosing the entire document directly, resulting in the leakage of the sensitive personal information it contains.

3.3 Lack of Data Masking and Security Protection Mechanisms

The primary challenge in protecting sensitive personal information is its identification [8]. While technical safeguards are a crucial pillar of personal information protection, grassroots administrative agencies currently face widespread issues such as a lack of data masking technology, weak security management, and insufficient staff training. Consequently, the technical capabilities for personal information protection struggle to meet practical demands.

First, there is a lack of de-identification technology. Grassroots administrative agencies lack awareness and technical capabilities regarding de-identification and have not strictly followed the requirements of government data de-identification standards to process personal information using technical methods such as de-identification, partial masking, and anonymization. Second, security management is weak. The security protection capabilities of government information disclosure platforms are insufficient; they have not established sound mechanisms for reviewing, retaining, monitoring, and deleting published information. Some platforms have security vulnerabilities, making them susceptible to cyberattacks and leading to the illegal acquisition of disclosed personal information. Additionally, expired information that has been disclosed is not promptly removed, creating a long-term risk of data leakage. Some information remains published far beyond the statutory retention period without any measures being taken to take it down or delete it. Third, there is a lack of staff training. Administrative agency personnel are unfamiliar with relevant laws and regulations—such as the Personal Information Protection Law and the Regulations on Government Information Disclosure—as well as data de-identification technical standards. They hold the erroneous mindset of "prioritizing disclosure over protection" and lack both a sense of responsibility and professional competence regarding personal information protection.

3.4 Obstructed Remedial Pathways for Rights Violations

A sound remedial mechanism is essential for safeguarding citizens' personal information rights. However, the current remedial mechanisms for personal information protection in government information disclosure suffer from difficulties in initiating remedies, ambiguous judicial review standards, and limited effectiveness. As a result, citizens find it difficult to obtain effective remedies when their personal information rights are infringed.

First, difficulties in initiating remedies. When citizens discover that their personal information has been unlawfully disclosed, they lack convenient channels for filing complaints, reports, or requests for correction or deletion. Administrative agencies have not established dedicated platforms for personal information protection complaints and reports, and the procedures for accepting and handling such cases are irregular and inefficient. Additionally, in administrative reconsideration and administrative litigation, plaintiffs must prove that their "legitimate rights and interests have suffered actual harm," which is difficult to demonstrate. As a result, many citizens are unable to initiate remedial procedures due to their inability to provide sufficient evidence. Second, judicial review standards are ambiguous. When adjudicating cases involving personal information protection in government information disclosure, courts lack uniform standards for defining core concepts such as "personal privacy," "public interest," and "differentiated treatment," resulting in a prominent phenomenon of inconsistent rulings in similar cases. Third, the effectiveness of remedies is limited. When adjudicating such

cases, courts often rule that the administrative agency's actions were unlawful and order the agency to rectify them, but they lack substantive remedies such as ceasing the infringement, deleting information, compensating for losses, or eliminating the adverse impact. Even when administrative agencies are ordered to rectify their actions, they often merely delete the relevant information without compensating the rights holder for the harm suffered, making it difficult to effectively safeguard citizens' personal information rights.

4. Pathways to Improving Personal Information Protection in Government Information Disclosure

Through systematic design involving legal amendments, detailed regulations, and improved procedures, we must explore a dynamic balance between data sharing and protection, thereby providing institutional support and legal safeguards to promote the orderly sharing of government data and strengthen the development of a digital government [9].

4.1 Unifying Standards for Identifying Personal Information and Tiered Protection

The key to resolving the issue of vague conceptual definitions lies in standardizing conceptual connections, establishing clear criteria for identifying personal information and a tiered protection system, and clarifying the boundaries between disclosure and protection.

First, standardize conceptual integration. Based on the Personal Information Protection Law, revise the Regulations on the Disclosure of Government Information to replace the term "personal privacy" with "personal information," and clearly define the scope of personal information in the context of government information disclosure: any information capable of identifying a specific natural person, including name, date of birth, ID number, biometric information, address, phone number, email address, health information, location data, and financial information. At the same time, clearly distinguish the boundary between personal information and information that has already been lawfully disclosed to prevent administrative agencies from abusing protection provisions to evade their disclosure obligations. Second, establish a "three-dimensional" determination standard. In line with practical needs, establish a "three-dimensional" determination standard comprising subjective intent, objective privacy, and harmful consequences to clarify the scope of personal information protection. Third, clarify the boundaries of public interest. Strictly limit the scope of application of the "public interest exception," restricting it solely to situations involving major public safety, significant social interests, and critical livelihood safeguards; when applying the public interest exception, the principle of proportionality must be followed, selecting the disclosure method that causes the least infringement on personal information, and prohibiting the broad application of the public interest exception clause [10].

4.2 Establishing a Comprehensive Review and Differentiated Handling Procedure

A sound procedural mechanism is key to regulating the information disclosure practices of administrative agencies and preventing the leakage of personal information. It is necessary to establish a comprehensive procedural regulatory system across three levels: the reviewing entity, the review process, and disclosure management.

First, establish a dedicated reviewing entity. A Review Committee for Information Disclosure and Personal Information Protection should be established to be responsible for identifying sensitive information, conducting legality reviews, performing de-identification reviews, and approving disclosures, thereby ensuring the professionalism and independence of the review process. Second, improve the pre-disclosure review process. All information that administrative agencies intend to disclose must first be reviewed by the Review Committee or a dedicated reviewer to determine whether it contains personal information, and to clarify the source, type, and scope of the personal information involved. For government information containing personal information, the agency must seek the data subject's opinion in writing, clearly informing them of the scope, method, duration, and risks of disclosure. If the data subject fails to respond by the deadline, consent to disclosure shall be deemed denied; Differentiated processing procedures: For government information containing a mix of personal and public information, sensitive content must be stripped, deleted, or de-identified before disclosure; where such information cannot be separated, it shall

generally not be disclosed or only the non-sensitive portions shall be disclosed; Public interest justification procedures: Where disclosure of personal information under the public interest exception is proposed, expert deliberations must be organized, reasons must be publicly announced, and public oversight must be accepted to ensure that the determination of public interest is lawful and reasonable.

4.3 Strengthening Data De-identification and Security Capabilities

Enhancing technical safeguards is a critical measure to prevent personal information leaks at the source. This requires aligning with government data de-identification standards, comprehensively implementing de-identification technologies, improving platform security capabilities, and strengthening staff training.

First, comprehensively implement de-identification technologies. Develop a nationally unified "Technical Standard for De-identification of Personal Information in Government Information Disclosure," clarifying the principles, methods, and operational norms for de-identification. Mandate that administrative agencies adopt standardized de-identification technologies when disclosing government information containing personal information, enabling the automatic identification and batch de-identification of sensitive information to improve efficiency and accuracy. Second, enhance platform security capabilities. Build a secure and controllable government information disclosure platform to prevent cyberattacks and unauthorized access; establish a dynamic monitoring mechanism for disclosed information to regularly identify risks of information leaks and promptly rectify non-compliant disclosures; strengthen platform upgrades and maintenance to promptly patch security vulnerabilities, ensuring the platform's security and stability.

4.4 Remedial Mechanisms: Ensuring Accessible Channels for Personal Information Rights Remedies

Ensuring unobstructed channels for redress serves as the final line of defense for safeguarding citizens' personal information rights. It is necessary to establish convenient administrative remedies, comprehensive judicial remedies, and all-encompassing oversight mechanisms to ensure that rights holders can obtain effective redress when their rights are infringed.

First, facilitate administrative remedies. Establish a nationwide unified platform for complaints and reports regarding personal information protection, implementing a working mechanism featuring centralized acceptance, time-limited resolution, and public feedback to facilitate citizens' reporting of illegal disclosures of personal information. Second, improving judicial remedies. First, plaintiff eligibility should be relaxed: as long as personal information has been unlawfully disclosed, the rights holder may file an administrative lawsuit without needing to prove actual harm, thereby lowering the threshold for initiating remedies. Second, judicial review standards should be clarified. When adjudicating cases, courts should focus on whether administrative agencies identified the personal information, fulfilled review procedures, performed de-identification, and complied with the principle of public interest. This will unify adjudication standards and reduce the phenomenon of inconsistent rulings in similar cases; Third, strengthen substantive remedies. When rendering judgments, in addition to confirming the illegality and ordering rectification, courts should, based on the rights holder's claims, order the administrative agency to cease the infringement, delete the information, compensate for losses, and eliminate the adverse impact. Courts should support injunctive and restorative remedies to ensure the effectiveness of the relief.

5. Conclusion

Information disclosure by administrative authorities and personal information protection are complementary and in dynamic balance. The former is the foundation for the construction of a rule-of-law administration, while the latter is the bottom line for the protection of citizens' rights and interests. The two are unified in the goal of building digital administration and rule-of-law administration. In current practice, there are dilemmas including ambiguous concepts, procedural deficiencies, insufficient technology, weak accountability, and inadequate remedies. These problems stem from imperfect institutions, inadequate coordination of legal norms, and ineffective implementation. To resolve such dilemmas, a full-chain protection mechanism should be established featuring

"clear standards, rigorous procedures, technological support, definite accountability, and unimpeded remedies". By unifying definition standards, improving review procedures, strengthening technical protection, perfecting the accountability system, and unblocking remedy channels, a balance between the right to know and personal information rights and interests can be realized.

In the future, with the improvement of supporting norms and technological progress, the protection of the two will move toward standardization, legalization and intelligentization, so as to achieve the organic unity of transparent exercise of public power and protection of citizens' private rights, and provide support for the construction of rule-of-law administration and smart society.

References

[1] Zhang Tao. Typological Reconstruction of the Legal Basis for Administrative Organs' Processing of Personal Information. Law and Social Development, 2026, 32(02): 53-73.

[2] Xie Dengke. Legal Risks and Prevention and Control Systems in the Processing of Sensitive Personal Information. Journal of Southwest Minzu University (Humanities and Social Sciences Edition), 1-10.

[3] Li Weihua. A Study on the Protection of Personal Privacy Information in Government Information Disclosure in the Era of the Civil Code. Politics and Law, 2021, (10): 14-24.

[4] Liu Liu. On Conflicts of Interest and Balancing in Personal Information Protection in China. Dongyue Collection, 2025, 46(09): 183-190.

[5] Wang Fang, Zheng Yuxin, Zhu Hongzhi. Protection of Personal Privacy in Government Information Disclosure: A Study Based on the Context of Major Public Health Emergencies. Journal of Information Resource Management, 2022, 12(05): 25-40.

[6] Fan Mingzhi. On the Separation of Data Security and Personal Information Protection Regulatory Systems. Political and Legal Studies, 2025, (04): 94-109.

[7] Zhang Tao. The Refined Application of the Principle of Proportionality in the Processing of Personal Information by Administrative Agencies. Journal of Huazhong University of Science and Technology (Social Sciences Edition), 2025, 39(06): 48-59+96.

[8] Yang Shangdong. On the Protection of Sensitive Personal Information in Government Information Disclosure in the Big Data Era. Studies in Administrative Law, 2025, (04): 101-114.

[9] Meng Qinguo, Zhou Qianyu. Institutional Improvements for Personal Information Protection in Government Data Sharing. Henan Social Sciences, 2025, 33(11): 59-69.

[10] Kong Fanhua. Protection of Personal Privacy in Government Information Disclosure. Studies in Administrative Law, 2020, (01): 17-29.

