Article

On the Protected Legal Interest of the Crime of Infringing upon Citizens' Personal Information: With the Right to Informational Self-Determination at Its Core

Yiming Lu[1,*]

[1] Beijing Normal University, Beijing, China
* Correspondence: Yiming Lu, Beijing Normal University, Beijing, China

Abstract: The crime of infringing upon citizens' personal information in China's Criminal Law has played a significant regulatory role in safeguarding individual rights in the information age. However, long-standing theoretical disagreements over its protected legal interest have directly undermined the precision of legal application and the depth of scholarly inquiry. Through a systematic doctrinal analysis of the nature of the legal interest, this article argues that the core protected legal interest should be citizens' right to informational self-determination. Personal information possesses an independent legal nature, characterized primarily by identifiability, which distinguishes it from the mere concept of data. Among the competing theoretical positions, the supra-individual legal interest theory encounters difficulties in systematic positioning and ambiguity of the legal interest itself, while the individual legal interest approach aligns more closely with the crime's normative placement. Within individual legal interest doctrines, the theories of personal dignity and personal freedom prove excessively abstract; the privacy right theory fails to meet the demands of protection in the digital age; and the personal information right theory, though reasonable, still requires further refinement to distill its essential core. As the substantive kernel of the right to personal information, the right to informational self-determination is grounded in both comparative law origins—particularly the landmark ruling of the German Federal Constitutional Court in the 1983 Census Case—and domestic legal norms. It furnishes a clear theoretical benchmark for interpreting the crime's constituent elements and delimiting the scope of criminalization, thereby enabling precise protection of citizens' personal information rights and interests.

Keywords: personal information protection; informational self-determination; individual legal interest; criminal law; legal interest theory

Received: 24 May 2026
Revised: 14 July 2026
Accepted: 28 July 2026
Published: 03 August 2026

1. Introduction

The rapid advancement of digital technology has ushered human society into an era characterized by pervasive data generation and information exchange. The convergence and application of technologies such as network infrastructure, intelligent systems, and large-scale data analysis have elevated data to a foundational element supporting socio-economic progress. While widespread data utilization has improved operational efficiency and reshaped daily life patterns, it has simultaneously intensified risks to personal privacy. Unauthorized and unlawful activities involving personal data continue to emerge, threatening individual rights, property security, and societal stability. In this context, developing a coherent legal framework for safeguarding personal data presents a shared priority for judicial systems globally.

To address mounting concerns over personal data protection in the digital environment, China adopted a legislative sequence wherein provisions addressing serious violations were introduced prior to comprehensive civil-level frameworks. Initial statutory provisions targeting misuse of personal data appeared in 2009, followed by consolidation and expansion in 2015, broadening scope and reinforcing enforcement mechanisms [1]. Subsequent enactments established foundational principles across multiple domains, progressively building a layered system for personal data governance.

Yet this sequencing approach has given rise to conceptual and operational challenges [2]. Discontinuities between early provisions and later-developed normative foundations have led to divergent interpretations of key concepts and inconsistent application in practice. Judicial handling of cases involving personal data often overlaps with matters concerning data integrity and asset-related misconduct. Precise delineation—both between conduct warranting formal intervention and that falling outside its scope, and among distinct categories of regulated conduct—requires foundational clarity regarding the underlying protected interest. Academic discourse has advanced several interpretive models, including those centered on private sphere integrity, autonomous control over personal data, and exclusive entitlements to data use. This diversity underscores both the urgency of conceptual alignment and the difficulties inherent in achieving consensus—difficulties that directly affect consistency in practical implementation.

Defining the protected interest carries decisive implications beyond theoretical debate: it shapes how statutory elements are construed and determines which forms of conduct fall within the intended scope of intervention. Should autonomous control over personal data be affirmed as the central protected interest, then any behavior constituting a material impairment of that autonomy may be considered eligible for formal response under applicable norms. To ensure coherence in protection, it is essential—following systematic evaluation of existing interpretive positions—to affirm autonomous control as the primary protected interest, thereby offering a consistent analytical foundation for case assessment and strengthening the overall effectiveness of protective mechanisms [1].

This article applies doctrinal legal methodology, integrating structural interpretation, cross-jurisdictional comparison, and normative analysis to examine the foundational interest underlying personal data protection [3]. The inquiry unfolds in five stages: first, clarifying the conceptual boundaries and juridical nature of personal data; second, distinguishing between interests grounded in individual autonomy and those rooted in collective considerations; third, evaluating competing models situated within the individual-interest paradigm; fourth, affirming autonomous control over personal data as the central protected interest; and finally, outlining the theoretical and operational consequences of this determination.

2. The Concept and Legal Attributes of Personal Information

2.1. Defining Citizens' Personal Information

In the legal framework governing personal data, the conceptual definition has evolved progressively. A key judicial interpretation defines citizens' personal information as various types of information recorded in electronic or other forms that can identify a specific natural person either independently or in conjunction with other data, or that reflect the activities of such a person. Other regulatory instruments have also provided definitions from distinct perspectives, with minor differences in phrasing, yet all centering on the criterion of identifiability [4].

Drawing upon these provisions, personal information may be understood as a symbolic system linked to a particular individual, reflecting distinctive personal attributes and exhibiting identifiability—encompassing details related to identity, employment, family, assets, health, and similar domains [2]. Some academic viewpoints suggest that certain categories of data—such as authentication credentials—lack inherent identifiability and thus fall outside the scope of protected personal information under legal frameworks focused on individual identification. However, this view is increasingly untenable. In contemporary digital environments characterized by widespread real-name registration requirements, authentication credentials are functionally integrated with personal identity; platforms such as widely used messaging and payment services exemplify this linkage. Consequently, such data remain consistent with the foundational principle of identifiability, aligning with prevailing scholarly understanding.

The identifiability standard serves a pivotal function: it establishes the essential link between information and a particular natural person—the very basis for recognizing such information as an object of personality-related rights. Identifiability manifests both directly and indirectly. Under current data-processing capabilities, indirect identification has become markedly more effective; disparate and fragmented data points, when aggregated and analyzed, can precisely pinpoint individuals. This technical reality supports a proportionate broadening of the protective scope applicable to personal information.

2.2. Distinguishing Personal Information from Personal Data

Having clarified the basic meaning of personal information, it is necessary to further distinguish between personal information and personal data. The wave of digitization has propelled personal information through a "datafication" transformation, with the carrier of personal information shifting from traditional tangible objects to the intangible form of electronic data [3]. Some scholars suggest that the distinction between personal information and personal data arises from inconsistent translations of foreign literature, and that there is no essential difference between the two. This view is questionable.

Personal information possesses distinct legal significance and cannot be simply equated with data. Under current legislative frameworks, personal information is defined primarily by its identifiability, encompassing both personality-related and property-related attributes, and constitutes specific personality interests. Personal data, by contrast, refers to unprocessed original records stored in electronic information systems; such records lack autonomous legal status when detached from their operational environment [5]. Personal information, conversely, represents processed, meaningful content derived from personal data and may retain its informational value even when represented in non-electronic forms. Regulatory provisions differentiate between network-related data and personal information, underscoring that protection focuses on the substantive informational content rather than raw system-stored records.

This conceptual distinction carries significant practical implications for legal application. In judicial practice, offenses involving unauthorized acquisition or misuse of personal information are sometimes conflated with those concerning unauthorized access to or manipulation of computer-stored records, largely due to conceptual overlap between personal information and data. Treating the two as interchangeable would undermine the distinct legal function of personal information protections [3]. From the perspective of protected interests, certain offenses safeguard the integrity of information systems and data management processes, whereas others safeguard individuals' personality interests. Fundamental differences exist in both the nature of protected interests and the mechanisms of infringement. Clarifying this boundary is essential for accurate classification of offenses and appropriate delineation of legal responsibility.

2.3. The Legal Attributes of Personal Information

Whether personal information constitutes a legal interest or a right is assessed according to three criteria: first, whether the interest protected by law possesses distinctiveness; second, whether differing protective approaches yield materially divergent outcomes; and third, whether analogous provisions exist in relevant foreign legal frameworks [6]. Applying these criteria supports recognizing personal information as a right, a position adopted in this analysis.

Personal information lacks physical form and cannot be possessed or controlled through material means; its regulation relies entirely on legal mechanisms—specifically, prohibitions against unauthorized collection, processing, and use. The structure of the personal information right, which grants designated civil subjects authority to manage and restrict unlawful interference, aligns it with rights that operate universally within the civil domain, such as personality-related rights [7]. As a distinct civil entitlement, the personal information right falls within the category of specific personality rights, grounded fundamentally in "identifiability" and "autonomous, exclusive management," and is not derivative of privacy rights, public interests, or data security considerations.

In terms of its essential nature, the personal information right encompasses both personality-related and property-related dimensions, with the former consistently prevailing [7]. Any property-related value arises from its personality foundation, reflecting the commercial application of personality-related protections—such value cannot exist independently of those foundational interests. This conceptual framing is essential for clarifying the scope of legal protection: safeguarding personal information centers on upholding personality-related interests, while property-related effects constitute incidental consequences of violations, rather than primary objects of legal protection.

3. The Debate between Individual and Supra-Individual Legal Interests

Theoretical controversies regarding the protected legal interest of the crime of infringing upon citizens' personal information are generally classified into three categories: individual legal interest, supra-individual legal interest, and dual legal interest. The debate between individual and supra-individual legal interests constitutes the central theoretical issue [8]. From perspectives including systematic positioning and clarity of legal interest, the individual legal interest theory better conforms to the normative positioning of this offense.

3.1. Systematic Positioning Indicates Protection of Individual Legal Interests

The offense of infringing upon citizens' personal information is situated within Chapter IV of the Specific Provisions, titled 'Offenses Infringing upon Citizens' Personal Rights and Democratic Rights.' According to the principle of analogous protected interests, offenses in this chapter all involve violations of citizens' personal rights and democratic rights. While differing views exist regarding the precise categorization of such rights, the scope of protected interests consistently centers on individual citizens rather than public or aggregated interests [5]. This structural placement reflects a deliberate legislative determination concerning the nature of the interest safeguarded by this offense.

A perspective suggesting that this offense involves multiple protected interests—including personality, property, and societal interests—lacks sufficient grounding. First, the defining feature of personal information is its capacity for individual identification; conduct violating this norm directly affects specific persons, and its inherent personality dimension is indisputable, whereas any property-related implications arise solely from the commercial application of personality interests and do not constitute independent property rights [9]. Second, societal considerations represent cumulative consequences of harm to individuals, not autonomous protected interests. Third, adopting a multiple-interest framework risks overextending legal application, contradicting the principle of statutory restraint. Fourth, judicial guidance consistently emphasizes individual rights as the central criterion, with thresholds for legal intervention calibrated according to the extent of individual harm. Accordingly, the multiple-interest interpretation is not tenable, and the protected interest remains strictly individual in nature.

From the standpoint of systematic interpretation, the principle of analogous protected interests serves a foundational interpretive function [8]. The legislative decision to locate a particular offense within a defined chapter signals an authoritative judgment about the character of the interest it safeguards. Placing the offense of infringing upon citizens' personal information within the same chapter as offenses targeting bodily integrity and autonomy—such as intentional infliction of serious bodily harm—reinforces its classification as one that protects individual legal interests.

3.2. Public Information Security and Exclusive Information Rights Are Both Untenable

The concept of public security in legal theory pertains to societal interests involving life safety, physical health safety, and major property safety for unspecified or numerous individuals [10]. The protected interest of this offense does not align with that definition: the subjects affected may be specific individuals or a limited group, and information security falls outside the conventional scope of 'security.' While misuse of personal information may indirectly and potentially lead to personal or property harm, such consequences are neither immediate nor inherent to the act itself. Consequently, characterizing the protected interest as public information security misapplies the concept of public security and lacks theoretical foundation.

The central flaw in the public information security framework lies in conflating secondary risks—such as downstream harms arising from unlawful dissemination of personal information—with the primary legal interest directly affected by the conduct [11]. Although large-scale unauthorized circulation may elevate the likelihood of subsequent offenses, this effect remains indirect and derivative; it cannot constitute an independent protected interest. In legal analysis, the protected interest must correspond to the object directly targeted by the prohibited conduct, not to remote or contingent outcomes.

The exclusive information right framework suffers primarily from ambiguity regarding the rightful subject of personal information rights. Such rights properly reside with the individual to whom the information relates. By extending rights to certain information processors, this framework inappropriately recasts entities that bear obligations into holders of rights. This conflation creates two interrelated difficulties: first, existing legislation does not confer exclusive rights over held information upon network platforms; second, treating such rights as shared interests risks transforming legal protections into instruments for asserting corporate control over data, thereby undermining the fundamental objective of safeguarding individual rights.

3.3. The Perspective of Natural Crimes Versus Statutory Crimes Corroborates the Individual Legal Interest Position

The essence of the debate between individual and supra-individual protected interests concerns whether the offense of infringing upon citizens' personal information should be classified as a natural offense or a statutory offense. Generally, natural offenses target individual protected interests, whereas statutory offenses primarily safeguard collective or systemic interests. A line of reasoning holds that this offense exhibits features of both categories—termed a 'natural offense with statutory characteristics'—based on three considerations: first, within the legislative structure, it appears in a section traditionally associated with offenses aligned with widely accepted ethical norms; second, the requirement of 'violation of state provisions' does not undermine its foundational nature as a natural offense, reflecting instead a formal codification of pre-existing moral wrongs; third, the inclusion of organizational liability does not transform the offense into a statutory one [11]. Given its classification as a natural offense, the primary protected interest is properly understood as individual in nature. This reasoning is logically coherent and academically sound.

From an ethical standpoint, the act of unlawfully acquiring, selling, or disclosing others' personal information carries inherent moral censure, requiring no legal definition to be judged negatively [12]. Such conduct fundamentally undermines personal dignity and impairs autonomy—wrongs that would be widely condemned across societies, even in the absence of specific legal frameworks for personal information protection. This intrinsic ethical reproach constitutes a hallmark of natural offenses.

While certain formal elements—such as the stipulation of 'violation of relevant state provisions'—introduce statutory features, these are procedural and structural in nature, not substantive [13]. They do not alter the core character of the offense as one directed against individual protected interests.

3.4. Supra-Individual Legal Interests Fail to Meet the Requirement of Legal Interest Definiteness

Proponents of supra-individual legal interests often highlight risks to public order arising from large-scale unlawful circulation of personal information; however, this perspective fails to adequately justify why conduct involving only specific natural persons' information also satisfies thresholds for legal intervention. Judicial guidance indicates that certain acts—such as transferring personal information yielding illicit proceeds exceeding 5,000 yuan, or repeating such conduct after prior administrative sanction—are classified as warranting heightened scrutiny [14]. These situations may involve exclusively individual information rights without any demonstrable effect on broader societal arrangements. Interpreting acts directed at particular individuals as inherently endangering generalized interests undermines the centrality of citizens as holders of information rights and introduces both conceptual inconsistency and normative imbalance.

A foundational requirement of contemporary legal interest theory is the clarity and specificity of protected interests [15]. A principal role of the legal interest concept is to supply substantive criteria for interpreting statutory provisions and to constrain the overreach of enforcement authority. Should the interests safeguarded under statutory provisions be reduced to vague formulations such as 'disruption of social arrangements' or 'generalized harmfulness,' then all offenses could be subsumed under overly broad categories, rendering the legal interest concept ineffective for interpretive precision or boundary maintenance. The validity of supra-individual considerations must remain grounded in their capacity to support the protection of individual rights; extending their application beyond this function not only compromises the principle of statutory clarity but may also generate tensions between personal entitlements and abstract societal considerations.

With regard to the requirement of specificity in assessing infringement, supra-individual legal interests frequently exhibit indeterminacy and lack empirical grounding, hindering precise measurement and consistent evaluation of harm. By contrast, infringement assessments concerning individual legal interests are more tangible and delineated, enabling judicial bodies to apply provisions accurately and allowing individuals to anticipate legal consequences with reasonable certainty—thereby aligning with the principle of clarity in legal regulation. Consequently, legal interest analysis should move away from supra-individual frameworks and refocus on the direct safeguarding of citizens' personal information rights and interests.

4. Critical Examination of Doctrines within the Individual Legal Interest Framework

Having established the basic position of individual legal interests, it is necessary to further examine various specific doctrines within this framework to identify the legal interest content that most accurately reflects the protective essence of the offense. Within the individual legal interest theory, perspectives range from general personality rights—such as personal dignity and personal freedom—to specific personality rights, including privacy rights, personal information rights, and the right to informational self-determination. A critical examination of each doctrine is required to ascertain whether the right to informational self-determination occupies a core position.

4.1. Critical Assessment of the Personal Dignity and Personal Freedom Theory

Scholars advocating the personal dignity and personal freedom theory argue that, given the placement of this offense within the specific provisions of the relevant legal framework and its proximity to offenses concerning correspondence autonomy, the protected interest should align closely with those offenses—namely, individual dignity and autonomy [16].

This perspective faces challenges due to its reliance on highly abstract notions of dignity and autonomy as the core protected interests for offenses involving unauthorized handling of personal data—a domain already subject to precise, functionally tailored safeguards. Dignity and autonomy are foundational principles enshrined in overarching legal instruments, carrying broad normative scope. Treating such generalized personality interests as direct objects of protection under specialized legal provisions risks overextending interpretive boundaries. While dignity serves as a unifying principle within frameworks governing personality interests, where concrete, enumerated rights exist and are operationally defined, invoking overarching principles without reference to those specific protections dilutes the precision required in legal application. In jurisdictions where the concept of informational self-determination has matured, recourse to generalized dignity or autonomy principles is generally considered unnecessary and jurisprudentially unsound.

The dedicated legal framework governing personal data explicitly specifies actionable rights—including rights to notice, consent, access, duplication, and erasure—rather than relying on abstract formulations of dignity. As a complementary regulatory instrument, the specialized legal provisions governing data-related offenses must reflect consistency with prior legislative design. To satisfy the requirement of conceptual specificity, protected interests must be sufficiently delineated and contextually grounded; overly broad constructs like dignity and autonomy lack the definitional clarity needed to support consistent, objective assessment of violations involving personal data [17].

4.2. Critical Reflection on the Privacy Right Theory

The privacy right theory holds considerable influence in Chinese academic discourse and appears to be gaining prominence. This theory posits that the protected legal interest of the offense is the privacy right among democratic rights, defining personal information narrowly as information concerning private life that can identify or relate to an individual's identity. Some analyses suggest that recent legislative developments reflect a value orientation emphasizing the protection of personal privacy [18].

Although the privacy right theory possesses certain historical rationality, it increasingly struggles to meet the practical demands of personal information protection in the digital era [19]. The conceptual linkage between personal information and privacy originated from their substantial overlap during early internet development. However, with the rapid advancement of digital technologies, information exchange and sharing have become pervasive, and the distinction between personal information and privacy has grown increasingly pronounced. Privacy fundamentally centers on the non-public nature of private life, embodying characteristics of solitude and non-disclosure; by contrast, digitized personal information is often widely disseminated and circulated, exhibiting attributes markedly different from those of traditional privacy.

Moreover, the privacy right theory fails to adequately address the protection of personal information that has already been made publicly available. Information disclosed by authorized public institutions—though falling outside the domain of privacy—remains personal information and warrants legal protection. If privacy were the sole protected interest, then lawful acquisition and use of such officially disclosed information would not constitute infringement, contradicting established legislative frameworks and judicial interpretation. Legal provisions also treat personal information and privacy as distinct, parallel concepts, underscoring their conceptual separation.

From the perspective of rights structure, privacy primarily functions as a negative defensive right, centered on the liberty of being left undisturbed; in contrast, the personal information right encompasses both negative defense and positive control. The information subject not only possesses the right to prevent unauthorized interference but also retains authority to determine how personal information is collected, used, and shared. Construing privacy as the sole protected interest cannot fully accommodate violations involving the positive control dimension—particularly cases where information is lawfully obtained but subsequently employed beyond the scope of consent or authorization [5]. Thus, the privacy right theory exhibits inherent limitations in protective coverage.

4.3. Affirmation and Limitations of the Personal Information Right Theory

Within the category of specific personality rights, the personal information right framework is more appropriate than the privacy right framework. Traditional approaches to privacy protection have proven inadequate for safeguarding digitized personal information in the data-driven era, prompting a gradual legislative and doctrinal shift toward recognizing personal information as a distinct protected interest. This framework conceptualizes the personal information interest as the lawful capacity of natural persons to control, manage, and prevent unauthorized use of their personal information, incorporating elements such as the right to determine information disclosure, the right to access one's own information, and the right to request correction of inaccurate information [20]. Legislative recognition of personal information within the personality rights provisions affirms its foundational status as a personality-related interest.

The strength of this framework lies in its alignment with evolving societal and technological realities, treating personal information interests as autonomous rights rather than derivative aspects of privacy [21]. This approach corresponds closely with the trajectory of domestic legal development and effectively accommodates the growing volume of non-sensitive personal information requiring protection in practice. Relative to the privacy-based framework, it offers broader protective coverage and a more nuanced articulation of associated entitlements.

Nonetheless, certain conceptual limitations remain. The personal information interest encompasses a range of distinct entitlements; if treated as a unified legal interest under enforcement mechanisms, further clarification is required regarding which components constitute the central, most critical interests warranting prioritized safeguarding. As the ultimate legal safeguard, enforcement measures must be applied selectively—focusing on those interests whose violation poses the most significant risk to individual autonomy and dignity. For instance, rights related to access and correction are typically addressed effectively through administrative or civil channels and generally do not necessitate intervention by coercive legal instruments. Thus, while the framework correctly situates personal information within the domain of personality-related interests, its core protective priorities require precise delineation.

5. The Core Status of the Right to Informational Self-Determination

Based on a systematic review of doctrines within the individual legal interest framework, it can be concluded that the right to informational self-determination constitutes the core protected legal interest in cases involving infringement of citizens' personal information. This right forms the substantive foundation of the personal information right and is supported by established comparative legal principles as well as domestic legal provisions, offering clear theoretical guidance for judicial application [3, 16].

5.1. The Right to Informational Self-Determination as the Core of the Personal Information Right

The core of the personal information right is the right to informational self-determination—that is, the information subject has the fundamental right to determine whether their personal information can be known by others and the manner and scope of such knowledge [4]. The essence of infringing upon the right to informational self-determination lies in undermining personal freedom in decision-making, which constitutes a key focus of legal protection. In other words, the right to informational self-determination and the personal information right are complementary; the former constitutes the core content of the latter. The various specific powers encompassed by the personal information right are essentially concrete manifestations of the right to informational self-determination at different stages: the right to know is the prerequisite for self-determination, the right to decide is the central element, the rights to access and copy support the exercise of self-determination, and the rights to correction and deletion serve as remedial safeguards.

The theory of the right to informational self-determination has deep roots in comparative legal scholarship. In one major jurisdiction, this concept emerged from foundational principles concerning human dignity and personality rights, was formally affirmed through a landmark judicial ruling in 1983, and later codified in national data protection legislation. That judicial ruling emphasized that the core purpose of the right is to safeguard individuals against constraints on personal development arising from uncontrolled collection, storage, use, and sharing of personal information. This theoretical framework has significantly influenced the evolution of personal information protection regimes worldwide.

In another major jurisdiction, personal information protection has historically been situated within broader privacy frameworks. However, recent judicial developments have expanded the conceptual boundaries beyond traditional notions of seclusion, with courts recognizing a functional equivalent to self-determination—namely, the right to control how personal information is handled. Although the theoretical foundations differ across these systems, they converge substantively through shared emphasis on individual agency in managing personal information.

5.2. The Normative Foundations of the Right to Informational Self-Determination

Within the current legal framework, although the term 'right to informational self-determination' does not appear as an explicit concept, its underlying principles are reflected across multiple regulatory instruments. A foundational requirement for information handling is established through the principle of informed consent; comprehensive civil legislation and dedicated personal information regulations jointly establish a continuum of control rights for individuals, covering all stages from collection and use to retention and deletion. These provisions collectively articulate the essential nature of personal information interests as self-determination—namely, the individual's authority to decide the scope, timing, recipients, and methods of disclosure or disposal of their personal information.

Specifically, regulatory requirements mandate individual authorization as a prerequisite for acquiring or sharing personal information—affirming the principle of autonomous choice. Further, where processing relies on individual authorization, such authorization must be freely given and clearly expressed following full disclosure of relevant matters. This establishes a procedural framework centered on transparency, awareness, and voluntary agreement, reinforcing the principle that individuals retain decision-making authority over their personal information [10]. Consequently, while the precise terminology remains unstated, the substance of informational self-determination is embedded in statutory provisions and constitutes a central element of personal information protection.

The normative basis for this right operates across multiple layers of regulation. At the highest level of legal hierarchy, foundational values concerning human dignity and personal autonomy serve as guiding principles. At the civil regulatory level, personality-related protections recognize the civil character of informational self-determination. At the operational level, specialized regulations set forth detailed rules and enforcement mechanisms. Together, these interlocking provisions provide a robust foundation supporting protective measures within broader legal frameworks.

5.3. The Logic of Criminal Law Protection of the Right to Informational Self-Determination

A provision in the national legal framework establishes an offense related to unauthorized handling of personal information, taking as its protected interest the individual's right to informational self-determination as established in prior legal instruments, and imposing legal consequences for unlawful acquisition, sale, or provision of such information. Through a formulation that references compliance with state-level requirements, the legislative design creates coherence between this provision and the foundational principles governing informational self-determination set forth in earlier legal instruments. When individuals process personal information without authorization and contrary to the expressed or implied will of the information subject, they not only depart from the boundaries established by legal instruments on personal information handling but also trigger legal accountability due to the substantive impairment of the individual's right to informational self-determination.

Recognizing the right to informational self-determination as the central protected interest carries significant theoretical and practical significance. First, this right offers a consistent conceptual foundation for interpreting the elements of the offense. Whether the conduct involves unauthorized acquisition, sale, or provision, the essential illegality stems from disregard for the information subject’s autonomous decision-making and interference with their authority to control and determine the use of their personal information. Grounding interpretation in this right enables precise clarification of the unlawful nature across different conduct types, thereby promoting consistency in judicial application. Second, this right supports principled delineation of the scope of legal accountability. Conduct that overrides the information subject's will and undermines their authority over personal information possesses a sound basis for inclusion within the scope of legal accountability, while also allowing for thoughtful consideration of additional conduct categories where appropriate.

Moreover, affirming the centrality of the right to informational self-determination facilitates alignment between this provision and earlier legal instruments. Prior legal frameworks structure personal information governance around this right, and this provision safeguards the same interest, reinforcing coherence across the legal system. At the same time, the definitional clarity of the right supports the principle of proportionality in legal accountability. Intervention through formal legal measures is warranted only when the infringement reaches a level of seriousness that exceeds the capacity of civil or administrative mechanisms to provide effective redress.

In summary, the interest protected by the offense concerning unauthorized handling of personal information is an individual interest, grounded substantively in the right to informational self-determination. This understanding aligns with the systematic role of legal provisions and ensures normative continuity with earlier legal instruments, offering clear interpretive direction for application. Importantly, anchoring the offense in this right provides a sound conceptual basis for evaluating additional conduct categories: any action that substantially impairs the right to informational self-determination may be considered for inclusion within the scope of legal accountability, provided it meets thresholds of seriousness and necessity [15].

6. Conclusion

The severe challenges faced by personal information protection in the digital era have placed higher demands on the responsive capacity of legal frameworks governing conduct. The debate over the protected interest of offenses involving unauthorized handling of personal information, while appearing on the surface as a divergence of doctrinal perspectives, fundamentally reflects underlying complexities concerning the legal character of personal information, the interplay among different layers of legal instruments, and the role of interest-based analysis in normative design. Through systematic review of existing doctrines, this article identifies the protected interest of such offenses as individuals' right to informational self-determination. This position resolves systemic inconsistencies and conceptual ambiguity associated with collective-interest approaches and avoids the theoretical limitations of individual-interest models—namely, unduly narrow scope or excessive abstraction.

Grounding the protected interest in the right to informational self-determination aligns with established principles in comparative legal systems and coheres with domestic normative structures. Consent-based mechanisms, rights conferred upon data subjects, and comprehensive procedural controls across relevant legal instruments all center on this right. As the final layer of normative enforcement, legal frameworks governing serious misconduct adopt this right—established in prior regulatory instruments—as their core protected interest. This linkage is effectuated through provisions referencing compliance with applicable requirements, thereby supporting coherence across the legal system.

At the level of application, the right to informational self-determination offers clear interpretive guidance for assessing conduct elements. The unlawful nature of acts such as unauthorized acquisition, transfer, or disclosure of personal information stems from disregard for the subject's autonomous choices and interference with their ability to control and manage their own information. This standard provides clarity and practical utility, supporting consistent judicial evaluation. In defining the scope of intervention, this approach preserves appropriate restraint: minor interferences amenable to resolution through civil or administrative measures fall outside its domain, while novel forms of interference that meaningfully impair informational autonomy retain a sound basis for inclusion within the scope of serious legal response.

Looking ahead, ongoing advances in digital technology will continue to raise new considerations for legal responses to personal information handling. Challenges arising from algorithmic processing, cross-jurisdictional data movement, and heightened safeguards for sensitive categories—including biometric identifiers—require theoretical frameworks capable of adaptive engagement. A structure anchored in the right to informational self-determination upholds foundational commitments to individual dignity and autonomy while allowing measured flexibility in implementation. This provides a stable conceptual foundation for refining protective mechanisms over time. Such an approach supports balanced outcomes—ensuring robust safeguards for personal information interests without impeding technological progress.

References

1. Z. Guo, J. Hao, and L. Kennedy, "Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law," *Comput. Law Secur. Rev.*, vol. 52, p. 105928, 2024.
2. Z. Guo, "Criminalisation of the illegal use of personal data: comparative approaches and the Chinese choice," *Humanit. Soc. Sci. Commun.*, vol. 12, no. 1, p. 782, 2025.
3. L. Zhang, "'Personal information of privacy nature' under Chinese Civil Code," *Comput. Law Secur. Rev.*, vol. 43, p. 105637, 2021.
4. J. B. Jacobs and E. Larrauri, "Are criminal convictions a public matter? The USA and Spain," *Punishm. Soc.*, vol. 14, no. 1, pp. 3–28, 2012.
5. J. Fan, "An Analysis of the Criminalization of Insult-Based Cyber Violence," *Law Sci.*, vol. 4, p. 755, 2025.
6. R. S. Sergent, "Fourth Amendment Model for Computer Networks and Data Privacy, A," *Va. Law Rev.*, vol. 81, p. 1181, 1995.
7. T. Yunfeng, "The Influence of the Personal Information Protection Law on Crime Evaluation under the Principle of Law Unity," *China Legal Sci.*, vol. 11, p. 110, 2023.
8. C. Lou, "Public or privacy? Dual process theory and fair use of disclosed personal information in Chinese judgments," *Tsinghua China Law Rev.*, vol. 16, p. 51, 2023.
9. S. D. Hampton, "Sleeping Giant: The Ninth Amendment and Criminal Law," *Sw. Univ. Law Rev.*, vol. 20, p. 349, 1991.
10. M. Messika, "Cybercrime and computer criminal law: typologies, prosecution and challenges in contemporary digital environments," *Tribunal de Justicia*, vol. 3, no. 2, pp. 107–119, 2026.
11. O. A. A. Francia, M. Nunez-del-Prado, H. Alatrista-Salas, and J. G. R. Alvarado, "Legal analysis of the nature of synthetic data: Personal data, anonymous data, or a sui generis category?," *Comput. Law Secur. Rev.*, vol. 62, p. 106379, 2026.
12. X. Yu and Y. Zhao, "Dualism in data protection: Balancing the right to personal data and the data property right," *Comput. Law Secur. Rev.*, vol. 35, no. 5, p. 105318, 2019.
13. T. R. Akash, N. J. Sany, L. Akter, and S. A. Sarna, "Privacy-preserving technique in cybersecurity: Balancing data protection and user rights," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 4, pp. 248–263, 2025.
14. X. Wang, "The Three-Tier Structure and Protection Mechanism of Personal Information Rights," *SWUPL Sci. Technol. Law Rev.*, vol. 2, p. 103, 2026.
15. J. E. Cohen, "Examined lives: Informational privacy and the subject as object," *Stan. Law Rev.*, vol. 52, p. 1373, 1999.
16. K. Swarts, "Selling Ourselves: A Critical Analysis of POPIA in the Age of Synthetic Data Markets," 2026.
17. R. Turner, "Employer Liability under Title VII for Hostile Environmental Sexual Harassment by Supervisory Personnel: The Impact and Aftermath of Meritor Savings Bank," *Howard Law J.*, vol. 33, p. 1, 1990.
18. H. Chang, "Privacy Accountability Management Framework for Data Controllers Operating across Asia," SSRN, 2014. [Online]. Available: https://ssrn.com/abstract=2523755
19. G. Hornung and C. Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination," *Comput. Law Secur. Rev.*, vol. 25, no. 1, pp. 84–88, 2009.
20. A. Rouvroy and Y. Poullet, "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy," in *Reinventing Data Protection?*, Dordrecht, Netherlands: Springer Netherlands, 2009, pp. 45–76.
21. P. K. Masur, "How online privacy literacy supports self-data protection and self-determination in the age of information," 2020.