Reflection on and Systematic Coordination of the Imputation Principles for Civil Liability in Personal Information Infringement Cases

Wenqi Du*

Hebei GEO University, Shijiazhuang City, 052161, China
**Corresponding author: 18238921570@139.com*

Abstract: *In the digital era, the infringement of personal information has become increasingly prominent, posing profound challenges to the principles of civil liability imputation. Traditional fault-based liability faces issues of ineffective relief and prevention due to the difficulties for information subjects in providing evidence and the challenges in assessing systemic risks. While no-fault liability can strengthen relief, it may lead to controversies such as the overgeneralization of liability and the stifling of innovation. A single imputation principle is insufficient to address the structural contradictions arising from the diversity of infringement forms, the complexity of causation, and the rigidity of exemptions from liability. This article posits that, based on reflecting on the limitations of existing principles, efforts should be directed toward constructing a layered, dynamic, and internally coordinated imputation system. This system allocates differentiated imputation principles based on the types of rights and the level of risks. By optimizing the core function of the presumption of fault principle and designing internal linkage mechanisms, such as dynamic conversion of imputation, coordinated burden of proof, and tiered exemptions, it aims to achieve the organic unification and systematic reconstruction of multiple values in tort law, including compensation, deterrence, and prevention.*

Keywords: *Personal information infringement; Imputation principles; Systematic coordination; Presumption of fault; Risk allocation*

Introduction

The legal protection of personal information rights and interests faces dual challenges in terms of substantive norms and procedural remedies. Among these, the appropriate configuration of civil liability imputation principles constitutes a core legal technical issue affecting the practical effectiveness of relief. Existing research predominantly engages in binary discussions that choose between fault-based liability and no-fault liability. This approach fails to adequately address the novel legal characteristics presented by personal information infringement, such as the compound nature of infringed objects, the procedural nature of infringing acts, and the technological asymmetry involved. Consequently, a significant tension exists between theoretical frameworks and judicial needs. This tension not only weakens the protective capacity of tort law regarding personal information rights and interests but also undermines the stability of behavioral expectations in data circulation and utilization. Therefore, it is of significant theoretical value and practical necessity to systematically reflect on the application dilemmas of traditional imputation principles. Moving beyond the debate over principle selection, exploring a civil liability imputation system that coordinates with the overall legal order of personal information protection—one that is both logically coherent and practically adaptable—is essential. This endeavor also represents an inevitable requirement for tort law to adapt to the development of the digital society.

1. The Theoretical Basis and Current State Examination of Imputation Principles for Personal Information Infringement

1.1 Limitations of Applying the Traditional Fault-Based Liability Principle in the Realm of Personal Information Infringement

1.1.1 The Structural Conflict Between Evidentiary Difficulties and Ineffective Relief

Personal information processing activities are characterized by high technological complexity and procedural opacity, with their operations under the unilateral control of the information processor. As the disadvantaged external party, the information subject finds it difficult to penetrate the algorithmic black boxes and system architecture to obtain direct evidence proving the processor's intent or negligence. Infringement often manifests in forms such as covert data aggregation, biases in automated decision-making, or systemic security flaws, far removed from the direct observability of traditional physical infringements. The imposition of the full burden of proving fault on the information subject essentially makes their procedural rights incapable of supporting substantive relief. This leads to the basic function of tort law—compensating for damages—failing in practice, creating a structural imbalance in litigation. This imbalance stems not only from the unequal technical capabilities of the parties but is also rooted in the inherent opacity and closed nature of the information processing architecture itself. Consequently, proving the element of fault becomes, in most scenarios, an impossible task, thereby undermining the foundational premise of the right to remedy[1].

1.1.2 The Functional Incongruence Between the Behavioral Evaluation Paradigm and the Prevention of Systemic Risks

The traditional fault-based liability principle focuses on the negative evaluation of specific, individual acts of infringement. However, the typical risks associated with personal information infringement often originate from a failure to establish organizational and technical security safeguards commensurate with the risks across the entire lifecycle of data processing. For instance, damages caused by lax default settings, inappropriate retention policies, or a lack of anonymization can be attributed to deficiencies in the state of systemic compliance, rather than to an isolated, blameworthy "act." The behavior-oriented framework for fault evaluation struggles to effectively encompass this type of "unlawful state" or "systemic misconduct." Consequently, the law's functions of preemptive risk regulation and damage prevention are significantly weakened, failing to adequately address the forward-looking requirement of "protection by design" emphasized in personal information protection.

1.2 Introduction of the No-Fault Liability Principle from a Risk Allocation Perspective and Its Theoretical Controversies

1.2.1 The Justification for Imputation Based on Risk Source and Benefit Attribution

According to the theory of risk allocation, entities that continuously engage in personal information processing activities are the creators and primary beneficiaries of this socially necessary risk. Following the legal principle that "where there is benefit, there lies responsibility," it aligns with distributive justice for them to bear the typical risks of harm associated with these activities. No-fault liability anchors the basis for imputation on the inherent dangerousness and beneficial nature of the activity itself, rather than on subjective fault. This directly eliminates the evidentiary difficulties faced by the information subject in an asymmetrical relationship, ensures the effectiveness of relief channels, and, through a cost internalization mechanism, incentivizes processors to make optimal investments in risk prevention and control, which is theoretically more efficient. This approach shifts the focus of tort law from the subjective mental state of the actor to an objective evaluation of the social utility and cost burden of the risky activity itself, reflecting the law's readjustment of the relationship between social production and risk distribution.

1.2.2 Potential Conflict Between Liability Overgeneralization and Industry Incentives

Criticisms primarily focus on the liability overgeneralization potentially induced by no-fault liability and its suppressive effect on industrial innovation. If applied indiscriminately and uniformly, it could lead to a widespread increase in compliance costs, imposing undue burdens on technology startups or non-profit research institutions. Furthermore, without a clear boundary of liability and a reasonable system of exemptions from liability, no-fault liability tends to inappropriately expand the scope of compensation. This may incorporate damages not directly or necessarily caused by the processing activities, thereby undermining the logical foundation of causation in tort liability. It also

risks excessively dampening the reasonable utilization of data resources and stifling the vitality of technological innovation.

1.3 Intrinsic Tensions Between the Current Imputation Principle System and the Characteristics of Personal Information Rights and Interests

1.3.1 Fundamental Contradiction Between the Composite Nature of Rights and the Singularity of Imputation Evaluation

Personal information rights and interests constitute a composite bundle of rights encompassing human dignity, personal freedom, property interests, and other elements. Infringement may cause simultaneous or separate damages of distinctly different natures, such as emotional distress, social discrimination, financial loss, or restriction of autonomous decision-making. Traditional imputation principles originated from the protection of relatively unitary legal interests; their constitutive elements and evaluation criteria were designed around specific types of damages. Faced with the infringement of composite rights and interests, any single imputation principle struggles to provide precise, comprehensive, and differentiated legal evaluations for the damages of varying natures involved. This can lead to insufficient relief or inaccurate evaluations.

1.3.2 The Prominence of Security Obligations and the Need to Expand Traditional Imputation Foundations

Modern personal information protection laws universally impose strict security obligations on information processors. These constitute proactive, organizational, and process-spanning standards of conduct and risk control duties. Their violation directly signifies the materialization of risk. Although the current imputation principle system, particularly fault-based liability, can interpret a gross violation of such obligations as presumptive fault through legal interpretation, its theoretical core remains anchored in the dichotomous framework of "fault" versus "risk." It has not sufficiently established "the breach of organizational duties" itself as an independent and significant foundation for imputation. This indicates that the existing system has not yet fully internalized the legal evaluation demands required by personal information protection—specifically, the need to assess continuous compliance states and proactive risk management[2].

2. Applicable Dilemmas and Structural Contradictions of Imputation Principles in Personal Information Infringement Cases

2.1 Conflict Between the Diversification of Rights Infringement Forms and the Unification of Imputation Principles

2.1.1 The Evaluation Dilemma of Non-Pecuniary Harm and the Weakening Link to the Fault Element

Non-pecuniary damages arising from personal information infringement, such as injury to personal dignity, disturbance of life tranquility, and damage to social reputation, find their legal foundation for compensation traditionally and closely linked to the subjective reprehensibility of the infringer. The traditional fault-based liability principle possesses a natural evaluative advantage in this domain, as its core lies in condemning the subjective state of the actor. However, in cases of personal information infringement, the severity of harm resulting from large-scale, systemic information breaches or misuse often does not perfectly correspond to the degree of subjective fault in any single processing act. For instance, a data leak caused by a complex system coupling failure may involve only minor negligence on the part of the processor, yet it can cause widespread social panic and severe individual psychological distress. In such scenarios, strictly adhering to the principle of proportionality between the degree of fault and the scope of liability may lead to insufficient relief. Conversely, relaxing the standard for determining fault to ensure adequate relief could distort the original intent of fault-based liability. This decoupling between the severity of the harm and the likelihood of subjective fault undermines the stable foundation of fault-based liability in evaluating such damages.

2.1.2 Remedial Obstacles for Economic Damages and the Prominence of Risk Allocation Demands

Parallel to non-pecuniary harm are the increasingly prominent economic damages, which include direct property losses (such as financial loss due to fraud), loss of transactional opportunities resulting from discriminatory automated decision-making, and defensive costs incurred to mitigate risks like

identity theft. This type of damage possesses a stronger objective and quantifiable nature. The key to its remedy lies in compensating the loss and preventing risks, rather than in strongly condemning the subjective state of the actor. The fault-based liability principle requires the injured party to prove the processor's fault, which presents a significant obstacle within the highly technical causal chain of economic harm. In contrast, the risk allocation theory offers greater explanatory power here: the processor benefits from data activities and is best positioned to control the associated economic risks through technical and managerial measures. Therefore, for economic damages, applying imputation principles oriented towards risk control (such as presumption of fault or no-fault liability) appears more justified and efficient. A single imputation principle cannot simultaneously optimize the evaluation and remedy for these two categories of damages — non-pecuniary and economic — which differ fundamentally in their value foundations and evidentiary paths.

2.1.3 The Dilemma of Choosing Imputation Principles in Cases of Intertwined Infringement Forms

In real-world personal information infringement cases, non-pecuniary harm and economic damages are often intertwined. For example, a leak of medical and health data may cause patients psychological anxiety while also leading to economic losses such as employment discrimination or insurance denial. Faced with such composite infringement, if adjudicators apply the fault-based liability principle, they may focus more on the non-pecuniary harm by emphasizing the evaluation of subjective culpability, thereby making the burden of proof and remedy for economic damages more difficult. Conversely, if they lean towards adopting no-fault liability to facilitate relief for economic damages, it may dilute the ethical condemnation warranted for the infringement of human dignity. Currently, there is a lack of an imputation mechanism capable of conducting dynamic evaluations, flexibly switching between, or applying principles in a tiered manner based on the dominant form of infringement or the core legal interest involved. Consequently, when confronted with composite infringement, regardless of which single principle is chosen, the adjudication inevitably falls into the dilemma of having to prioritize one value at the expense of the other[3].

2.2 The Difficulty in Establishing Causation and Its Impediment to the Functional Realization of Imputation Principles

2.2.1 Technical Evidentiary Challenges in Multi-Actor, Long-Chain Scenarios

The personal information ecosystem involves multiple actors such as data collectors, processors, analysts, and sharers, with data flow paths that are complex and opaque. A resulting harm may be caused by the joint or sequential actions of multiple processors, creating situations of multiple causes for a single effect or extended causal chains. As external parties, information subjects have almost no means to penetrate the technological black boxes to trace and prove which specific action by which processor(s) at which stage directly caused the final harm. For example, in cases of personalized pricing discrimination based on user profiling, proving that specific data aggregation or algorithmic models directly caused the price differential is extremely difficult from a technical standpoint. This technical evidentiary challenge causes the fundamental imputation logic of "the actor bears the responsibility" to fundamentally collapse at the operational level.

2.2.2 The Latent, Cumulative, and Uncertain Nature of Damages

Damages resulting from personal information infringement often do not manifest immediately; instead, they exhibit characteristics of latency, accumulation, and future risk. Once data is breached, the resulting harm may be exploited and become apparent only years later. Prolonged data surveillance and profiling can subtly influence an individual's development opportunities, with damages that are difficult to quantify concretely in the present. This "latent damage" or "risk-based damage" makes the traditional "but-for" causation test difficult to apply. When the damage has not yet materialized or merely constitutes a significantly elevated risk, it is challenging to establish causation legally. Consequently, the function of imputation principles is constrained to providing remedies for damages that have already occurred and can be clearly proven. It fails to effectively encompass the prevention of risks and the early intervention against potential damages, thereby weakening the law's capacity for forward-looking regulation[4].

2.2.3 The Erosion of Imputation Principle Functionality by the Rigid Allocation of the Burden of Proof

Whether under fault-based liability or no-fault liability, if the burden of proving causation is rigidly assigned entirely to the information subject, its practical effect is tantamount to nullifying the

imputation principles established in substantive law. Fault-based liability is difficult to invoke because the information subject cannot prove fault; while no-fault liability dispenses with the need to prove fault, if the burden of proving causation remains undiminished, the threshold for establishing liability remains prohibitively high. Therefore, the difficulty in proving causation constitutes a preliminary, common obstacle that may render any sophisticated design of imputation principles ineffective in judicial practice. To activate the intended functions of imputation principles, it is imperative to make corresponding adaptive adjustments to the element of causation, particularly its rules for allocating the burden of proof. This could involve introducing presumptions of causation, lowering the standard of proof, or shifting part of the burden of proof. Otherwise, any discussion of systematically coordinating these imputation principles will lack a practical foundation.

2.3 Insufficient Coordination Between the System of Exemptions from Liability and the Value Objectives of Imputation Principles

2.3.1 Difficulties in Interpreting and Applying Traditional Exemptions from Liability in the Digital Context

When traditional exemptions from liability in tort law, such as force majeure, the victim's intent, or the fault of a third party, are transplanted into the context of personal information infringement, their connotations and applicable boundaries become blurred. For instance, what constitutes "force majeure" in the field of data processing? Are sophisticated cyberattacks by state-sponsored hacker groups equivalent in nature to the accidental exposure of a technical vulnerability? Does an information subject's "consent" to broad privacy terms in exchange for convenience constitute "victim fault" or assumption of risk? Under conditions of severe information asymmetry, the voluntariness and validity of such consent are inherently questionable. Mechanically applying traditional exemptions from liability may inappropriately relieve the information processor of responsibility or, conversely, due to overly strict interpretation, virtually eliminate the possibility of exemption, leading to absolute liability[5].

2.3.2 Conflict Between Typological Differences in Risk Activities and the Homogeneous Design of Exemptions from Liability

Personal information processing activities vary significantly in their associated risks. The public interest nature, probability of harm, and nature of potential damages differ greatly between data processing in clinical medical research and that in commercial targeted advertising. However, the current legal framework lacks a typified and tiered design for exemptions from liability that corresponds to these varying levels of risk and contextual differences. For high-risk activities (such as processing biometric data or medical and health data), it may be necessary to establish extremely stringent conditions for exemption. Conversely, for low-risk, public-interest activities, more reasonable room for exemption should be allowed. The current homogeneous design of exemptions from liability fails to achieve the differentiated policy objectives of rewarding compliance, encouraging beneficial data utilization, and severely punishing high-risk violations. This renders the imputation system rigid and lacking in responsiveness.

2.3.3 The Absence of Dynamic Compliance Efforts in the Evaluation of Exemptions from Liability

Modern personal information protection laws emphasize "privacy by design and by default" and impose continuous compliance obligations. The dynamic compliance efforts undertaken by processors to fulfill these duties—such as conducting regular security audits, adopting encryption technologies, and performing privacy impact assessments—should be reflected in the determination of their liability, particularly when assessing the existence of fault or eligibility for mitigated liability. However, the existing system of exemptions from liability predominantly consists of static, after-the-fact, "binary" judgments (e.g., whether an event constitutes force majeure). It fails to incorporate the processor's proactive, ongoing, and systematic efforts in risk prevention and control as a dynamic factor that could partially offset liability. This omission undermines the system's function of providing positive incentives for good compliance behavior. It also means that the outcome of liability imputation may not accurately reflect the processor's actual degree of culpability and level of risk control.

3. Constructing a Coordinated Framework for the Imputation Principles in Personal Information Infringement Cases

3.1 Tiered Allocation of Imputation Principles Based on Rights Types and Risk Levels

3.1.1 Identification and Matrix Formation of Infringement Types and Risk Levels

The prerequisite for tiered allocation is the clear classification of infringement objects and behavioral risks. Infringement types can be categorized based on their core legal interests into: "personality-centric infringement," focusing on human dignity and mental tranquility, and "property-autonomy infringement," characterized by property loss and impairment of autonomous decision-making. Concurrently, the risk level of information processing activities can be comprehensively assessed based on factors such as the sensitivity of the processed information (e.g., biometric, medical health, or location tracking information being high-risk), the scale and degree of automation of the processing behavior, and the openness of the processing scenario. By constructing a two-dimensional "rights type – risk level" matrix, differentiated default imputation principles can be matched to different combinations. This ensures that the assigned intensity of imputation is proportional to the importance of the legal interests being protected and the potential harmfulness of the behavior[6].

3.1.2 Differentiated Matching of Imputation Principles Based on the Layered Model

Under this layered model, the configuration of imputation principles adopts a graduated approach. For any type of infringement arising from processing activities involving core sensitive information and posing high risks, the application of no-fault liability or a reinforced version of the presumption of fault may be considered. The legal rationale lies in the fact that such activities create significant risks that society must strictly control. The processor, who enjoys substantial benefits and possesses absolute control, should bear the strictest liability to achieve the strongest deterrent effect. For "property-autonomy infringement" resulting from activities of general risk, the presumption of fault principle becomes the appropriate choice. It balances the evidentiary capabilities of both parties by inverting the burden of proof, focusing on compensating damages and internalizing the costs of risk. For scenarios involving low-risk activities or those primarily concerning "personality-centric infringement" without high risk, the system may revert to general fault-based liability, focusing on evaluating the actor's subjective culpability and ethical condemnation. This differentiated matching allows the tools of imputation to precisely target the core issues they are designed to address.

3.1.3 Theoretical Advantages of Layered Allocation: From Value Conflict to Functional Complementarity

The core advantage of the layered allocation strategy lies in its transformation of macro-level value conflicts into micro-level functional complementarity and synergy. It acknowledges that different imputation principles each have their own functional emphasis: no-fault liability excels at risk allocation and loss distribution; the presumption of fault is superior in resolving evidentiary difficulties under information asymmetry; and fault-based liability is precise in moral evaluation and behavioral guidance. By invoking different principles in different contexts, the system can more flexibly and accurately achieve multiple objectives such as compensation, deterrence, prevention, and education. This avoids the dilemma inherent to a single principle when confronting complex realities—being either "too rigid to be practical when applied universally" or "too weak to be effective in addressing all circumstances." Consequently, the imputation system itself gains greater explanatory flexibility and adaptability.

3.2 Optimization of the Presumption of Fault Principle and Its Functional Positioning within the Imputation System

3.2.1 Refined and Flexible Adjustment of the Allocation of the Burden of Proof

The traditional presumption of fault involves a simple inversion of the burden of proof, which may impose an undue burden on the processor in certain scenarios. The direction for optimization lies in refining and introducing flexibility into this mechanism. Specifically, the information subject should bear the initial burden of proof, demonstrating the existence of information processing activities, that they have suffered harm, and that there is a prima facie connection between the two. The burden of proof then shifts to the information processor, who must prove that they have fulfilled comprehensive security and compliance management obligations throughout the entire data processing lifecycle,

obligations commensurate with the declared risk level and nature of the processing. The "proof" required here is not merely self-certification of the absence of intent or negligence. Rather, it necessitates providing an evidential chain of organizational, procedural, and technical measures, such as privacy impact assessment reports, security audit records, and internal training materials. If the processor can sufficiently demonstrate that it has exercised "good governance" obligations, the presumption of no fault can be made; otherwise, the presumption of fault stands[7].

3.2.2 Deep Integration with Defenses Centered on "Fulfillment of Security Obligations"

The core essence of the optimized presumption of fault principle is a "presumption of duty breach." The processor's primary line of defense shifts from proving the abstract notion of "no fault" to demonstrating the concrete fact of "having fulfilled statutory security obligations." This redirects the focus of imputation from investigating subjective mental states to examining objective organizational conduct and compliance status. This shift holds dual significance: Firstly, it highly aligns with the principle of accountability emphasized in personal information protection legislation, creating effective resonance between civil imputation and public law compliance requirements. Secondly, it provides processors with clear behavioral guidance and a defined direction for exemption efforts, incentivizing them to establish and maintain an effective internal governance system, thereby achieving the legal effect of prioritizing prevention.

3.2.3 Functional Positioning as the System's "Regulator" and "Default Option"

Within the layered imputation system, the optimized presumption of fault principle should be positioned as a broadly applicable "default option" or "regulator." For the majority of cases falling within the intermediate spectrum of risk levels and infringement types, the presumption of fault provides a balanced and operable solution for imputation. Simultaneously, it can serve as a bridge connecting strict liability (no-fault liability) with more lenient liability (fault-based liability). In specific circumstances, by adjusting the standard of proof required for demonstrating "fulfillment of obligations" within the presumption—such as demanding a standard approaching "high probability" or merely requiring a "preponderance of evidence"—or by defining the substantive content of security obligations in legislation with varying degrees of strictness, the effect of the presumption of fault principle can be substantially aligned with either strict liability or fault-based liability. This enables a smooth transition and dynamic fine-tuning of imputation intensity across the system.

3.3 Construction of a Dynamic Imputation System and Design of Internal Linkage Mechanisms

3.3.1 Triggering and Conversion Rules for the Dynamic Application of Imputation Principles

The core of a dynamic system lies in establishing clear triggering and conversion mechanisms. For instance, when an information processor fails to fulfill special protection obligations stipulated by law regarding high-risk information, even if general fault-based liability or presumption of fault was originally applicable, the "severity of the duty breach" can trigger a conversion to a stricter imputation principle (such as reinforced application of presumption of fault or direct application of no-fault liability). Conversely, when a processor can prove not only compliance with basic obligations but also the adoption of industry-leading protective measures exceeding legal requirements, yet damage still occurs, it may, under specific conditions, be permitted to invoke more favorable exemption clauses or receive a mitigated quantification of liability. The rules governing such dynamic conversions should be transparent and based on the processor's specific conduct rather than its identity, ensuring the system's responsiveness and fairness.

3.3.2 Linkage Mechanism Between the Burden of Proving Causation and Imputation Principles

To overcome the difficulties in proving causation as discussed in Chapter 2, it is essential to design a linkage mechanism with imputation principles. In high-risk areas where no-fault liability or a reinforced presumption of fault applies, rules such as "presumption of causation" or "reduction of the burden of proof" may be introduced concurrently. Specifically, if the information subject proves that the damage occurred after the processor's high-risk activity under its control, and that the damage is of a type typically likely to result from such activity, the existence of causation is presumed. The burden of proof then shifts to the processor to rebut this presumption. This linkage combines the strictness of the imputation principle with an adjustment of the burden of proof, preventing the constitutive elements of liability from working against each other. It creates a synergistic effect to genuinely open up effective relief channels.

3.3.3 A Tiered System of Exemptions from Liability and the Incorporation of Dynamic Compliance

Finally, the dynamic imputation system needs to be matched with a tiered, scenario-specific system of exemptions from liability. This system should establish thresholds for exemption of varying strictness, corresponding to the different default imputation principles and risk levels. The key lies in formally incorporating the information processor's "dynamic compliance efforts" into the considerations for exemption or mitigation of liability. If a processor can demonstrate that it has established and continuously improved a data governance framework that meets or even exceeds industry standards, and that it promptly took effective remedial measures upon the occurrence of damage, these facts, while not necessarily leading to complete exemption, should constitute significant mitigating factors for reducing compensatory damages or avoiding punitive damages. This transforms the imputation system from a purely outcome-based liability framework to one that also evaluates behavioral processes. It encourages continuous, good-faith risk prevention and control, achieving a positive interaction between legal evaluation and behavioral incentives. Through the design of the aforementioned internal linkage mechanisms, the system of civil liability imputation principles for personal information infringement evolves from a rigid set of rules into an organic whole capable of self-adjustment, balancing principle with flexibility.

Conclusion

Reflection on the civil liability imputation principles for personal information infringement reveals that relying on any single principle to provide a comprehensive solution is impractical. The way forward lies in systematic and coordinated construction. This involves using the type of rights infringement and the risk level of information processing activities as fundamental evaluative dimensions to implement a refined, tiered allocation of imputation principles. This ensures that the intensity of imputation corresponds to the importance of the legal interests protected and the riskiness of the behavior. Within this system, an optimized presumption of fault principle should play a central, pivotal role. Its essence lies in the "presumption of duty breach," effectively bridging the evaluation of subjective culpability with the examination of objective compliance status.

The ultimate establishment of a dynamic imputation system relies on the synergistic design of internal linkage rules, such as flexible conversion mechanisms between imputation principles, coordinated adjustments to the burden of proving causation, and a tiered system of exemptions from liability that incorporates considerations of dynamic compliance. This system aims to shift from static rules to dynamic evaluation and from singular sanctions to pluralistic incentives, thereby constructing a more resilient legal equilibrium between the protection and utilization of personal information. Future research could build upon this foundation to further explore operational issues, including the specific quantitative standards for "risk levels," the precise triggering thresholds for conversions between different imputation principles, and objective metrics for evaluating dynamic compliance.

References

[1] Feng, Yaxiang. Research on Compensation for Damages in Personal Information Infringement within the Context of the Digital Economy. 2025. Harbin University of Commerce, MA thesis.
[2] Wu, Daoyan. Research on Legal Issues Concerning Civil Infringement of Sensitive Personal Information. 2025. Guizhou Normal University, MA thesis.
[3] Chen, Yu, and Zeng, Rongyu. "On the Imputation Principles and Application for Personal Information Infringement: A Study Based on Article 69, Paragraph 1 of the Personal Information Protection Law." Digital Economy and Law 01(2025):205-225+279-280.
[4] Dong, Chao. Research on the Determination of Personal Information Infringement by Mobile Internet Platforms. 2024. Guizhou Normal University, MA thesis.
[5] Li, Mingli. Research on Liability for Personal Information Infringement in the Digital Age. 2024. Hebei University of Economics and Business, MA thesis.
[6] Si, Qi. The Application of the Presumption of Fault Principle in Liability for Personal Information Infringement. 2022. Nanjing Normal University, MA thesis.
[7] Li, Ying. Research on Liability for Personal Information Infringement in the Civil Code. 2021. Liaoning University, MA thesis.