WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 9, Number 1, Year 2025
DOI: https://doi.org/10.62051/ijsspa.v9n1.20
Journal homepage: https://ijsspa.org

The Judicial Adjudication Logic of Data Privacy Cases from the Perspective of Basic Rights

Chang Qu

School of Law, Hunan Normal University, Changsha 410000, China

ABSTRACT

With the continuous technological evolution of the digital age, data privacy has become an integral part of citizens' basic rights and a key component. The continued expansion of data privacy rights on internet platforms poses new challenges to the traditional judicial adjudication framework. This article, approaching data privacy cases from a fundamental rights perspective, draws on the Civil Code and the Personal Information Protection Law as normative support, and draws on a sample of 576 judicial cases to systematically analyze the adjudication logic of data privacy cases. Regarding the definition of rights, it clarifies the fundamental right nature and dual validity of data privacy. Regarding infringement determination, it establishes a system of elements encompassing "illegality of conduct - consequences of damage - causation - subjective fault." Regarding procedural rules, it refines the tiered distribution standard for the burden of proof. Furthermore, in the process of balancing interests, it applies the principle of proportionality to reconcile the contradiction between rights protection and data utilization. This research reveals that current adjudication practice suffers from problems such as "different judgments in similar cases" and insufficient regulation of data privacy rights. Guiding cases are needed to unify adjudication standards and improve the path to rights redress. The conclusion is that only by integrating fundamental rights protection throughout the entire adjudication process can substantive justice in the judicial protection of data privacy be achieved while ensuring the orderly development of the digital industry.

KEYWORDS

Fundamental Rights; Data Privacy; Judicial Adjudication; Burden of Proof; Proportionality Principle.

1. INTRODUCTION

Against the backdrop of the accelerated evolution of the digital economy, data privacy has gradually evolved from a subsidiary interest of traditional privacy rights to an independent interest with fundamental rights attributes. According to judicial sample statistics, from 2016 to 2023, courts nationwide heard 576 personal information-related cases, with an average annual increase of over 30% in data privacy infringement cases. These cases demonstrate diverse infringing parties, concealed methods of infringement, and intangible consequences. From the CSDN user data leak to the mass exposure of hotel check-in information, such incidents not only threaten citizens' personal dignity but also continuously undermine the foundation of social trust. Traditional fundamental rights theory, centered on the "state-individual" binary framework, focuses on preventing infringement of rights by public power. However, in the digital age, the rapid rise of private social power, represented by internet platforms, has created an asymmetrical "platform-individual" relationship of dominance, posing dual challenges to the protection of fundamental rights: both theoretical adaptation and practical implementation. Although the Personal Information Protection Law has established a foundational regulatory framework for data privacy protection, judicial practice still presents challenges such as ambiguous rights definition, disorderly allocation of the burden of proof, and an

inappropriate balance of interests. For example, in the Wang case involving cross-border data, the court faced the challenge of balancing the fundamental rights of information subjects with the efficiency of international commercial transactions. The Wang case involving hotel information exposed the judicial difficulty of proving causation. Based on this, this article, approached from the perspective of fundamental rights, drawing on typical judicial cases and current legal norms, deconstructs the core elements of adjudicative logic in data privacy cases, analyzes prominent practical difficulties, and explores avenues for improvement. This article aims to provide theoretical references for judicial adjudication and promote a healthy balance between data privacy protection and the proper use of data.

2. DEFINING THE FUNDAMENTAL RIGHTS ATTRIBUTES OF DATA PRIVACY AND JUDICIAL RECOGNITION

The definition of data privacy rights is the logical starting point for judicial adjudication of data privacy cases. The key is to clarify whether data privacy possesses fundamental rights attributes and how to define the boundaries of its effectiveness [1]. Traditional fundamental rights theory centers on the vertical relationship between the state and the individual, focusing on preventing infringements of rights by public power. However, data privacy infringements in the digital age are more likely to stem from the manipulation of private social power by entities such as internet platforms. This requires adjudicators to break away from this traditional theoretical framework and explicitly recognize the fundamental right status of data privacy. From a normative perspective, while data privacy is not explicitly enumerated in the Constitution, it falls within the category of fundamental rights not enumerated in the Constitution. Article 39 of the Constitution, regarding the inviolability of the home, and Article 40 regarding the confidentiality of communications, provide superior legal support for data privacy protection. Article 1032 of the Civil Code establishes the right to privacy as a specific personal right, and the Personal Information Protection Law further details special protection rules for sensitive personal information, forming a clearly defined regulatory framework. In judicial practice, the Guangzhou Internet Court, in the Wang Mou cross-border data case, explicitly emphasized that the cross-border transmission of personal information must be based on the protection of the fundamental rights of the information subject, directly affirming the core nature of data privacy as a fundamental right. The extension of the validity of fundamental rights is a key component of adjudicative logic. Germany's theory of indirect effect of the objective value order and the United States' theory of state action offer approaches for resolving conflicts of rights between private entities. Chinese judicial practice tends to leverage the general provisions of the Civil Code to constrain private entities through fundamental rights [2]. For example, in the case of Luo v. a technology company, the court rejected the platform's defense of excessive collection of user profile information based on "business model requirements." This, in essence, is regulating the platform's data privacy rights through the radiating effect of fundamental rights. Current judicial understanding still has significant limitations: some courts pay insufficient attention to the fundamental rights nature of data privacy and, in balancing the interests of platforms and individuals, overly favor industrial development initiatives. To address this issue, adjudicators need to strengthen their understanding of fundamental rights and establish data privacy protection as a benchmark throughout the adjudication process.

3. JUDICIAL DETERMINATION OF THE ELEMENTS OF LIABILITY FOR DATA PRIVACY TORTS

Clarifying the elements of tort liability is the core logic of adjudication in data privacy cases. Judicial practice has developed specific rules based on the four elements of "illegal act - harmful consequences - causal relationship - and subjective fault," but adaptation to the digital technology landscape still

presents challenges. Determination of illegal acts must balance the necessity of protecting fundamental rights with the legitimacy of data utilization. While legal grounds under Article 13 of the Personal Information Protection Law constitute a barrier to illegality, their scope of application needs to be strictly limited. In the case of Mr. Wang v. an international hotel company, the court distinguished between cross-border data transfers: "contract performance" transfers exempted from separate consent because they matched the intended purpose, while "commercial marketing" transfers were deemed illegal because they exceeded the scope and lacked separate consent. In practice, courts often assess legality based on the scope of collection, purpose of processing, and method of notification, explicitly disapproving practices such as "blanket consent" and "vague notification." The determination of damages requires moving beyond traditional thinking regarding material damages. Data privacy violations often involve intangible damages such as loss of information control and impairment of mental well-being. Article 1182 of the Civil Code provides regulatory basis for this. In practice, even in the absence of explicit material losses, courts may determine mental damages based on the circumstances of the infringement. For example, several cases involving excessive data collection by apps have awarded plaintiffs compensation for mental damages. However, the standard for determining whether minor infringement constitutes damages is still underdeveloped and requires further clarification. Proving causation faces the challenge of "evidential distance": the technical and closed nature of data processing makes it difficult for plaintiffs to prove the direct source of the information leak. In the case of Wang Moumou v. Han Mou Hotel, the court dismissed the claim on the grounds of unclear causation because the leaked information was not the exclusive property of the hotel. Some courts adopt a "plaintiff's initial proof followed by defendant's rebuttal" model: after the plaintiff proves the defendant possessed the information and had leaked it, the defendant then has to prove that their actions were not related to the damage. The determination of subjective fault relies on objective criteria, focusing on whether there was a violation of the statutory duty of care. The presumption of fault principle in Article 69 of the Personal Information Protection Law reduces the burden of proof for plaintiffs, requiring defendants to prove they fulfilled their data security obligations to be exempted from liability. In practice, courts often examine fault based on data encryption, third-party audits, and vulnerability remediation. Platforms that fail to implement tiered protections are directly deemed at fault [3].

4. SPECIAL RULES FOR THE ALLOCATION OF THE BURDEN OF PROOF IN DATA PRIVACY CASES

The allocation of the burden of proof plays a decisive role in the outcome of data privacy cases. Due to the high technical barriers and disparate status of the parties involved, these cases require a departure from the conventional "he who asserts, must provide the evidence" framework and instead establish a specialized allocation mechanism that aligns with the protection of fundamental rights. The burden of proof for the defendant's tortious conduct adopts a "tiered" allocation model. Plaintiffs must first fulfill their initial burden of proof, proving that the defendant engaged in information collection and harmed their rights and interests. This can include submitting screenshots of app privacy agreements and records retained after information leaks. In the case of Pang Moumou v. an information technology company, after the plaintiff presented evidence proving that the defendant had collected their personal information and that the information had indeed been leaked, the court immediately ordered the defendant to provide a complete explanation of the information processing process to prove its innocence. This allocation approach resolves the plaintiff's evidentiary dilemma caused by "evidential distance" without unduly increasing the defendant's burden of proof, thus achieving a preliminary balance between the interests of both parties. The burden of proof for the fault element is reversed. Unlike general personal rights infringement cases, in data privacy cases, the burden of proof rests on the defendant to prove their own lack of fault. This rule is rooted in the original legislative intent of the Personal Information Protection Law, which is to correct the imbalance between information processors and information subjects. In practice, defendants are

required to provide documents such as data security management system documents, employee confidentiality training records, and regular security audit reports to demonstrate fulfillment of their statutory duty of care. If they fail to provide valid evidence, the court will directly presume fault. The burden of proof for damages and causation requires flexible adjustment. Regarding damages, plaintiffs can claim the infringing party's actual profits in lieu of their actual losses. If neither party can provide sufficient evidence to prove the amount of loss, the court may determine the amount of compensation at its discretion, taking into account the circumstances of the infringement. In determining causation, if the defendant possesses key evidence but refuses to produce it, the court may apply the evidentiary obstruction rule to presume causation [4]. For example, in a case involving an information leak on a social media platform, the court directly presumed an information leak because the platform refused to submit data operation logs without justifiable reasons. Current evidentiary rules remain difficult to apply: some courts differ in their definition of "preliminary evidence," with some requiring plaintiffs to clearly demonstrate the specific aspects of the information leak, while others require only that the plaintiffs provide evidence of damage to their rights and interests. This issue requires further clarification and refinement through judicial interpretation, standardizing the evidentiary requirements for different types of infringement.

5. JUDICIAL APPLICATION OF THE PROPORTIONALITY PRINCIPLE IN BALANCING INTERESTS

Data privacy, as a fundamental right, is not absolutely exclusive. Judicial adjudications must rely on the proportionality principle to reconcile individual rights, industrial development, and the public interest. This is the core manifestation of the social function of fundamental rights. The principle of proportionality, encompassing three sub-principles: appropriateness, necessity, and balance, underpins the legality review of the entire data processing process and serves as a key tool for balancing interests in adjudication. The principle of appropriateness requires that the purpose of data processing be compatible with the protection of fundamental rights. In judicial practice, courts must focus on examining whether data processing activities align with legitimate purposes and explicitly deny processing activities that exceed these purposes [5]. For example, in the Wang case involving cross-border data, the hotel's transmission of user information to fulfill an accommodation contract met the appropriateness requirement. However, the transmission of information to a third party for commercial marketing purposes was deemed unlawful due to improper purposes. This ruling, in essence, leverages the legitimacy of the purpose to establish a strong protective boundary for fundamental rights, preventing unnecessary interference with those rights. The principle of necessity requires that data processing be conducted in a manner that minimizes infringement on rights. Courts must examine the availability of less stringent alternatives when adjudicating. If an app can perform its service functions using non-private information but still collects sensitive information such as ID numbers, this violates the principle of necessity. In the case of Luo v. a technology company, the court rejected the platform's defense that the collection of user profile information was "necessary for personalized push notifications," explicitly stating that the platform failed to adopt a less intrusive processing method, highlighting the role of the principle of necessity in protecting rights. The principle of proportionality requires a balance between rights protection and data utilization. When public interests conflict with individual rights, it's necessary to examine whether the benefits of data utilization outweigh the harm to fundamental rights. For example, during the pandemic, courts generally recognized the public interest nature of health code data processing, but required the prompt removal of redundant information after processing to avoid excessive privacy violations. In cross-border data flows, as in the case of Wang, cross-border data transfers deemed "contractually necessary" were recognized, ensuring transaction efficiency without weakening rights protection. The current application of the proportionality principle remains flawed: some courts excessively favor corporate commercial interests in balancing interests and define "necessary scope" in an overly broad manner. This requires adjudicators to cultivate a mindset that prioritizes fundamental rights, making

the proportionality principle a rigid constraint on balancing interests and preventing rights protection from becoming a mere formality.

6. PRACTICAL DILEMMAS AND PATHS FOR IMPROVEMENT IN JUDICIAL LOGIC

While the current judicial adjudication of data privacy cases has established a basic framework, from the perspective of fundamental rights protection, issues remain such as ambiguous application of rules and inadequate remedies. Improvement in adjudicative logic is needed through standardized regulation, technical assistance, and mechanism optimization. Practical difficulties manifest themselves in three key areas: First, the phenomenon of "different judgments in similar cases" is prominent. For example, in determining "reasonable confidentiality measures" for trade secret data, some courts require strict protective measures such as physical isolation, while others only recognize the effectiveness of technical safeguards such as API access control, resulting in significant discrepancies in standards. Second, fundamental rights are insufficiently regulated over data privacy rights. Reviews of platform algorithmic decisions often remain at the level of formal compliance, failing to delve into the rationality and transparency of algorithmic models, making it difficult to effectively constrain platforms' control over data. Third, the number of remedies is limited. In judicial practice, damages are often the primary remedy, while the rights to deletion and correction are rarely invoked due to unclear applicable standards. This results in superficial protection of fundamental rights and stagnation in achieving substantive justice. Targeted breakthroughs are needed to improve the path forward. First, relying on guiding cases to unify adjudicative standards, the Supreme People's Court should issue guiding cases focusing on typical scenarios such as cross-border data transmission, algorithmic recommendation, and the reuse of public data, clarifying the applicable rules for infringement determination, the burden of proof, and the principle of proportionality [6]. For example, in the protection of trade secret data, the specific elements of "reasonable confidentiality measures" could be refined to include data encryption and tiered access. Secondly, we should establish a multi-tiered legal application system, establish the priority of the Personal Information Protection Law, link inter-enterprise data disputes to the Anti-Unfair Competition Law, and apply the Copyright Law when data constitutes a work, forming a "special law takes precedence, and related laws complement each other" approach. At the same time, we should improve the legal connection rules for anonymized data to fill the institutional gap between personal information and commercial data. Finally, we should strengthen technological empowerment and diversified remedies. Courts can establish a system of data security expert assistance to address technical fact-finding challenges; establish a remedy system that prioritizes cessation of infringement and supplements damages, and clarify the applicable conditions and enforcement mechanisms for the right of deletion. We should also promote the coordination of judicial protection and industry self-regulation, requiring platforms to establish a system for recording data processing records throughout the entire process. This will not only reduce the difficulty for parties to provide evidence but also prevent data privacy risks at the source.

7. CONCLUSION

The demand for protecting citizens' basic rights in the digital age necessitates the reconstruction of the judicial adjudication logic for data privacy cases. Combining normative analysis with case observation, the adjudication logic within the context of fundamental rights must begin with the characterization of data privacy rights, center on the examination of the elements of infringement, be supported by the allocation of the burden of proof, and utilize the principle of proportionality as a tool for balancing interests, ultimately forming a three-dimensional framework of "rights protection-risk prevention-value balance." This framework not only addresses the difficulty in adapting the traditional fundamental rights theory's "state-individual" binary framework to digital scenarios, but also precisely aligns with the legislative intent of the Personal Information Protection Law to

strengthen data privacy protection. From a judicial perspective, adjudicators must break away from traditional rights protection paradigms and fully recognize the regulatory effect of fundamental rights on data privacy rights (such as the right of internet platforms to control data). This approach is exemplified by reducing the plaintiff's burden of proof based on the presumption of fault and correcting the imbalance in subject status through the reversal of the burden of proof. At the same time, addressing issues such as "different judgments in similar cases" and the disordered balancing of interests, it is necessary to achieve a unified adjudication standard through the publication of guiding cases and the introduction of technical experts to assist in trials. Data privacy protection and the reasonable use of data are not mutually exclusive.The core task of judicial adjudication lies in clearly defining the legal boundaries of data processing, based on fundamental rights. In the future, as judicial interpretations of the Personal Information Protection Law are refined, adjudicative logic will need to be further refined: The definition of data privacy as a right must be clarified as encompassing both personal rights and property rights; the accountability process must strengthen transparency scrutiny of algorithmic decision-making; and the criteria for determining public interest must be refined in the balancing of interests. Only in this way can we effectively safeguard the realization of data privacy as a fundamental right and lay a solid legal foundation for the healthy development of the digital economy.

REFERENCES

[1] Li Demian. On the protection of personal information in cross-border data flow [N]. Science Herald, 2025-04-03(B02). DOI:10.28511/n.cnki.nkxdb.2025.000221.

[2] Brkan M. The essence of the fundamental right to privacy and data protection: getting out of the maze of the EU Court's constitutional reasoning [J]. German Law Journal, 2019, 20(6): 864-883.

[3] Pollicino O, Romeo G. The Internet and the Constitution: The protection of fundamental rights and constitutional adjudication in Europe [M]. Routledge, 2016.

[4] Zhu Xiaofeng. Study on the Constitutive Elements of Personal Information Infringement Liability [J]. Comparative Law Research, 2023, (04): 132-149.

[5] Fabbrini F. EU Charter of Fundamental Rights and Data Privacy: The Court of Justice of the European Union as a Human Rights Court [J]. Five Years of a Legally Binding Charter of Fundamental Rights (Oxford, Hart Publishing, 2015), iCourts Working Paper Series, 2015 (19).

[6] Ding Xiaodong. Legal Theory of the Relationship between Privacy Protection and Personal Information Protection - On the Application of the Civil Code and the Personal Information Protection Law [J]. Legal and Business Research, 2023, 40 (06): 61-74. DOI: 10.16390/j.cnki.issn1672-0393.2023.06.012.