Journal of Infrastructure, Policy and Development 2024, 8(12), 9253.
https://doi.org/10.24294/jipd.v8i12.9253

Article

Securing privacy in the digital age: The quest for judicial protection of personal information

Zhihua Chen[1], Ruiyu Geng[2], Zhenglin Jia[3], Hanbin Wang[4], Fangzhou Hu[1], Qianyi Cai[2,*]

[1] Wuhan University School of Law, Wuhan 430072, China
[2] Wuhan University Institute of International Law, Wuhan 430072, China
[3] University of Hamburg, Business Administration, Hamburg 20148, Germany
[4] The University of New South Wales, Kensington Campus, Kensington 1466, Australia
*** Corresponding author:** Qianyi Cai, fxycqy@whu.edu.cn

CITATION

Chen Z, Geng R, Jia Z, et al. (2024). Securing privacy in the digital age: The quest for judicial protection of personal information. Journal of Infrastructure, Policy and Development. 8(12): 9253. https://doi.org/10.24294/jipd.v8i12.9253

ARTICLE INFO

Received: 23 September 2024
Accepted: 15 October 2024
Available online: 4 November 2024

Abstract: Personal information is a vital productive commodity in the digital economy, and its processing has seen unparalleled transformations in both breadth and depth. This article proposes to enhance the legal remedies for personal information rights in contemporary China. Research has revealed multiple practical challenges in China's judicial practices, such as hesitance to prosecute owing to an absence of substantial legal foundation, improper distribution of the burden of proof, and inadequate integration of criminal-civil judicial safeguards for personal information. This paper advocates for China to elucidate the definition of personal information rights via legislation, enable the litigation of personal information infringement cases, and establish explicit criteria for their acceptance into judicial proceedings. Furthermore, China must develop an appropriate structure for distributing the burden of evidence. It must also use discretionary judgment to properly tackle the problems related to evaluating damages in instances of personal information violations.

Keywords: personal information; judicial remedy; burden of proof; integration of criminal-civil judicial

1. Introduction

In the digital economy's early development, concerns about personal information privacy began to surface but were not yet widely discussed. The research primarily focused on the legal dimensions of personal information, examining its correlation with privacy rights and its possible advantages and disadvantages within the digital economy. Some scholars believe that in China's future Civil Code, the right to personal information should be separately stipulated as a specific personality right rather than subordinate to the right to privacy (Wang, 2013). Some scholars believe the right to personal information is an independent personality right regarding legal attributes (Zhang and Han, 2018). Asserted that personal information rights include not just privacy but also the authority over and stakes in one's own information (Cheng, 2023). These findings provide a robust theoretical framework for the judicial safeguarding of personal information, emphasizing the need of preserving persons' dignity and economic interests about their data.

With the expansion of the digital economy and internet technologies, the safeguarding of personal information has gained paramount importance, resulting in more in-depth study. Researchers are constructing more robust frameworks for personal information protection. asserts that the collecting of personal information must adhere to the principles of informed consent, privacy, and need (Zhang, 2019).

Posits that anonymized user data need to be regarded as personal information to safeguard users' rights in profiling and tailored services (Ding, 2019). Addresses the need of explicit legal obligations to guarantee adherence to privacy legislation via administrative penalties (Chen, 2023). These studies assist judicial authorities in ascertaining legal liabilities and implementing appropriate sanctions for breaches of personal information.

Research on the protection of personal information in China is progressively implemented and assessed for efficacy. Researchers analyze both theoretical models and their empirical results. Emphasizes the need of risk mitigation in data processing (Zhang, 2023), while examines the circumstances in which legal injunctions should safeguard personal information rights (Yang, 2023). Examines the EU's strategy for managing cross-border data flows, offering lessons for China's policy (Xia, 2023).

Nonetheless, a significant portion of China's research is theoretical, often devoid of actual data and interdisciplinary viewpoints, so limiting its practical applicability. This article connects theory and practice by examining court decisions to inform the safeguarding of personal information and proposes measures to enhance its legal protection via civil legislation.

2. Background of judicial protection for personal information

The conventional legal remedy framework has challenges in addressing violations of personal information rights in the digital economy. With the rapid leap into the digital economy era, every aspect of citizens' activities can be converted into data through technological means. Generating personal information has become as natural and inevitable as breathing out carbon dioxide. As information exchanges among various entities proliferate, the ensuing disputes likewise diversify, complicating the resolution via conventional remedies for rights such as privacy and reputation. The protection of personal information has become a prominent concern. The conventional "rights-based remedy model" often proves inadequate in resolving the many issues about personal information. This deficiency underscores the practical requirement and urgency of judicial remedies designed for personal information interests.

Nevertheless, contemporary legal remedies encounter several obstacles. Firstly, there is a lack of adequate substantive legislation. The absence of explicit legal backing complicates people' ability to assert their rights in instances of personal information breaches, while courts often exhibit conservatism and caution in adjudicating these matters. Secondly, the distribution of the burden of evidence in situations of personal information violation is unjust. As evidence is often retained by data processors, conventional burden of proof regulations frequently disfavors data subjects in legal proceedings. Furthermore, in instances of personal information breaches, correctly quantifying the real damages incurred by the data subjects is sometimes challenging. The granted compensation is seldom enough to offset actual losses and legal expenses, hence reducing the attractiveness of judicial remedies. Last but not least, the integration procedures between civil and criminal court safeguards for personal information privacy remain inadequate. This flaw results in ineffective transitions between criminal and civil proceedings. As a result, these impacts both the efficacy

and effectiveness of court remedies.

3. Security risks to personal information in the digital economy context

In the contemporary digital economy, the aggregation and use of personal data by enterprises and platforms are becoming more prevalent, resulting in various information security vulnerabilities. These dangers may result in the illicit gathering and use of personal data, along with violations of personal information security. This chapter will examine several categories of dangers related to the management of personal information. Comprehending these threats is essential for safeguarding personal data and preserving confidence in the digital economy.

3.1. Risk of unauthorized collection of personal information

The unauthorized gathering of personal information encompasses two categories, such as unauthorized collection and excessive collection. The unauthorized collecting of personal information pertains to merchants or platforms acquiring customers' data without express authorization and neglecting to disclose the purpose of the gathered information. In 2021, XPeng Automobile Sales Service Co., Ltd. placed surveillance cameras in its shops and unlawfully gathered and uploaded over 400,000 face images without securing customer authorization or explicitly disclosing the objective of the gathering. Ultimately, the company was fined 100,000 RMB by the Market Supervision Administration of Xuhui District, Shanghai (People's Commentary, 2024).

The excessive gathering of personal information is prevalent among online businesses and platforms, often including the coercive acquisition of superfluous data. The EASYHOME created the Wodong App, which was publically reprimanded by the Ministry of Industry and Information Technology for excessive acquisition of personal data (MIIT, 2022). This privacy policy requires that users provide personal information, including their actual name, gender, date of birth, delivery address, contact information, address book, picture album, calendar, and location data. Providing this personal information is a mandatory step for using the APP. However, it fails to inform users of the purposes for which this personal information is collected, nor does it inform users of their right to refuse or disable authorization for such information. People believe that collecting, using, and sharing personal information may threaten their privacy (Boerman, 2021). The excessive accumulation of personal information heightens the potential of eventual abuse or data breaches, profoundly affecting consumer privacy and security.

3.2. Risk of misuse of personal information

With the development of the digital economy, the use of personal information has significantly broadened in both extent and depth. Commercial companies may use personal data for targeted advertising, marketing, and tailored recommendations. The improper use of personal information for purposes such as fraud, harassment, manipulation, or discrimination jeopardizes individual rights and freedoms. Personal information has progressively transformed into a commodity, marketed to advertising,

criminals, or other entities with certain objectives. The hazards of personal information abuse are intensified by big data analysis. At present, there are six categories of algorithms that influence the rights of information subjects, such as ranking algorithms, probabilistic algorithms, traffic algorithms, recommendation algorithms, price algorithms, and assessment algorithms (Shanghai Consumers Council, 2021). Among them, pricing algorithms are known as "big data price discrimination". The use of information processing technology for data analysis and unrestrained data mining influences the predictability of the information processing objective. This disrupts the context of information exchange and results in privacy encroachment (Zhang, 2023). Ultimately, this not only directly affects the rights and interests of the information subjects but may also jeopardize the stability of the digital and wider social economy.

3.3. Risk of personal information leakage

In the era of the digital economy, the collection and retention of personal data have grown more prevalent and widespread. Entities may gather, retain, and use personal data without consent or sufficient safeguards, resulting in violations of individual privacy. This may include sensitive personal identification information, financial particulars, and medical data. The disclosure of such information might result in identity theft and fraud. Furthermore, in the digital economy, big data analysis are extensively used to integrate personal information with other data sets, uncovering comprehensive insights and behavioral patterns about people (Xue, 2024). This facilitates the provision of individualized goods and services, although it also presents dangers of personal privacy being inferred and disclosed. Personal information is kept in databases and cloud services, which may possess security weaknesses or be prone to assaults. Hacking, data breaches, and system vulnerabilities may result in the theft, alteration, or abuse of personal information.

4. China's judicial protection of personal information

In China, the rapid advancement of the digital economy has made the legal need for personal information security more pressing. In recent years, the state has consistently enhanced the statutory protection of personal information. Nonetheless, safeguarding personal rights to information in legal practice continues to pose several obstacles. Prior to examining emerging trends and legal advancements, it is essential to comprehend the present condition of China's judicial system regarding personal information protection and the obstacles it encounters.

4.1. New trends: Personal information data protection

Personal information protection is supported by legislation, with protective measures increasing to unprecedented levels. In 10 November 2021, the PIPL was formally enacted, signifying a new era in the safeguarding of personal information. It emphasizes the authorized, reasonable, and essential aspects of personal information processing. This not only fortifies the safeguarding of personal information, protecting the security and privacy of personal data, but also aids in preserving public interest and social order. The legislation further elucidates the duties and responsibilities of personal information processors. These restrictions would significantly mitigate the

dangers of personal information leakage and abuse, hence augmenting the security of personal data.

As the "Civil Code" and the PIPL are increasingly enforced, lawsuits about personal information infringement are demonstrating new features. As the "Civil Code" and the PIPL are increasingly enforced, lawsuits about personal information infringement are demonstrating new features. The incidence of instances concerning personal information protection has significantly risen (**Figure 1**).

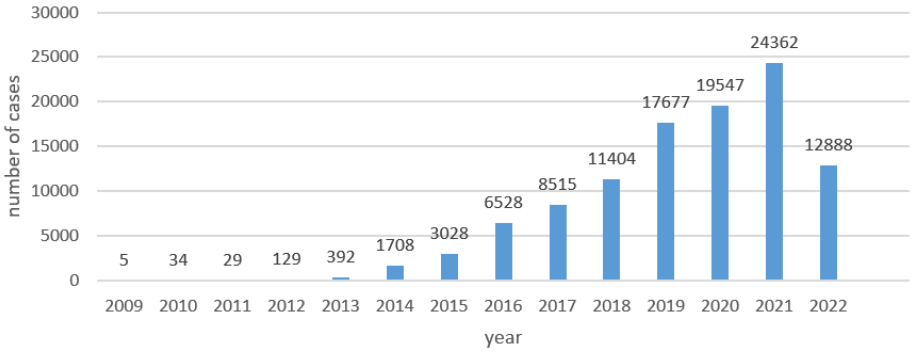

Figure 1. Civil cases on personal information protection[1].

[1]Source: China Judgment Documents Network, a full-text search using the keyword "personal information rights" and civil cases as the screening type on the "China Judgment Documents Network" yielded only 124 cases, as of 5 July 2023.

A visual analysis of the data indicates a year-on-year increase in legal disputes over personal information. The number of cases escalated from 29 in 2011 to approximately 20,000 by 2020, indicating an approximate 700-fold rise. Since 2013, the annual incidence of personal information civil claims has escalated by thousands, peaking in 2019 with a surge of almost 6000 instances in that year alone. In 2020, despite the pandemic significantly curtailing social activity, there was still a surge of over 1000 cases. The rising incidence of instances indicates the prevalent breaches of personal information in society and the increasing public desire for protective measures.

4.2. Legal gap: Ambiguous nature of personal information rights

China has enacted the Personal Information Protection Law, along with other laws. Nonetheless, in court practice, personal information rights have not yet been recognized as a separate civil right. Moreover, there is an absence of a definitive classification for the precise category of rights applicable to personal information.

This uncertainty renders ordinary persons inert in their pursuit of legal protection against unlawful use or breaches of their personal information, owing to the absence of a robust legal framework. Individuals often depend on other claims, such as privacy or defamation rights, to seek redress due to the ambiguous legal position of personal information rights. This indirect approach to redress may insufficiently safeguard the legitimate rights and interests of the data subjects. The scholarly agreement is that personal information rights fall within the classification of personality rights (Cheng, 2023). Individuals whose personal information has been compromised may pursue claims for personality rights or tort damages. Current judicial practice, however, demonstrates an inadequate comprehension of existing legislation, leading courts to

take a conservative, constrained, and cautious approach in addressing personal information issues. The uncertainty and fragmentation of private information also creates a wide gray space for judicial decisions (Li, 2020).

Investigations into personal information infringement cases indicate that, despite the prevalence of conflicts, instances particularly concerning personal information rights are very uncommon, highlighting a shortfall in court acknowledgment of these rights. Moreover, quantifying the precise losses resulting from the violation of personal information is challenging, so exacerbating and elevating the expenses associated with legal proceedings. These issues result in insufficient legal defense by persons confronting abuses of personal information rights, creating a gap between the legal remedies offered by the courts and the remedy sought in personal information disputes.

4.3. Inappropriate: Allocation of burden of proof

In disputes over tort compensation for the infringement of personal information rights, the plaintiff (the right holder of personal information) must prove the following essential elements: 1) the existence of an act by an information processor handling personal information; 2) the act of processing personal information has infringed their personal information rights; 3) that they have suffered damage; 4) a causal link between the information processing act and the infringement of rights; and 5) a causal link between the infringement of personal information rights and the damage incurred. Only then can the responsibility of the personal information processor for damages and the scope of such liability be ascertained (Civil Code of the People's Republic of China, Article 1165; Personal Information Protection Law of the People's Republic of China, Article 69).

However, in practice, the challenge for rights holders is obtaining precise information on the leakage of their personal data, given the majority of such data is managed by the information processors. Information processors have a technical advantage in possessing evidence and conducting investigations (Kong, 2022). This restriction significantly hinders their capacity to substantiate these factual features. Furthermore, rights holders have significant challenges in demonstrating that a party is highly probable to have disseminated personal information. Identifying the specific information processor responsible for the leak is almost an insurmountable challenge. Concurrently, violations of personal information might result in financial damage and induce emotional turmoil. Emotional discomfort is intangible and sometimes resists physical evidential presentation, complicating its quantification and legal proof (Li, 2023).

In situations of personal information infringement, the responsibility is on the information processors to demonstrate their lack of fault, rather than on the victims to establish the processors' liability (PIPL, Article 2). Nonetheless, the legals fails to define the manner in which data processors must demonstrate their compliance with requirements pertaining to information security or due diligence. Moreover, data collectors, controllers, and processors all face the potential danger of data leakage. However, requiring data processors to independently demonstrate the absence of such dangers undeniably increases their burden of proof. Both plaintiffs and defendants

evidently lack firsthand proof of the event's evolution, resulting in practical challenges in substantiating the criteria of infringement. Fundamentally, this evidentiary dilemma stems from the structural characteristics of personal information infringement in the digital age.

4.4. Fragile integration: Civil and criminal judicial protections

Within the existing legal framework in China, civil rules include personality rights, tort law safeguards, and the Personal Information Protection Law. In criminal law, the violation of individuals' personal information is a defined criminal offense, and there are administrative processes such as regulatory measures and public interest lawsuits (Zhou, 2021). Nonetheless, the extent of public interest lawsuits concerning personal information privacy is quite restricted. In some circumstances, prosecution authorities may begin a distinct kind of lawsuit (Supreme People's Procuratorate, 2020) . This transpires in instances of significant violations of individuals' personal data that considerably affect societal stability and the public interest. The authorities seek to completely safeguard the rights of victims via a mechanism termed criminal accessory civil public interest litigation. However, for general personal information protection disputes, civil judicial channels remain necessary for resolution.

Moreover, there are difficulties in managing civil public interest action related to criminal accessory involvement in personal information breaches. In instances of personal information breaches, the victims are usually many and frequently cannot be clearly recognized. The liable party, or infringer, often encounters legal responsibilities that are mostly restricted to public apologies and monetary restitution. Nonetheless, these compensations are often minor and administered by the prosecutorial authorities. This structure hinders the delivery of prompt and efficient legal protection for the persons concerned. One big problem is that criminal justice can't step in when someone violates the rights to personal information but doesn't break the law because the actions don't meet the criteria for a crime. The gap between civil and criminal justice protection for personal information is significantly widened by the cost associated with litigation. High legal fees deter individuals from pursuing lawsuits to protect their information rights. Consequently, many people refrain from suing to safeguard their personal information.

5. China's pathway: Enhancing the judicial protection of personal information in the digital economy

Despite China's initial establishment of a legal framework for personal information protection, the practical application of the legislation and its protective measures encounter several problems. To address these challenges, this chapter will take a series of measures.

5.1. Providing a clear legal framework for personal information protection

In order to assist data subjects in exercising their rights, it is essential to amend relevant laws. Implementing more extensive personal information protection rules and regulations is essential. These should explicitly describe the extent of protection for

personal information rights, specify acts of infringement, and establish the processes for claiming rights, therefore providing data subjects with a definitive legal foundation.

The existing legal framework (**Table 1**) must delineate more explicitly the rights and responsibilities pertaining to personal information protection and enhance the consequences for violations. First, the rights of data subjects must be explicitly delineated. This encompasses the authority to govern their personal data and make judgments about it. Moreover, data subjects need to possess the right to pursue compensation and remedy for any violations of their rights. Explicitly give certain rights, including the right to be informed, access, rectify, and delete personal information, while delineating the legal liability for infringing upon these rights (Xu and Quan, 2024). At the same time, the safeguarding of data subjects' rights to be informed and to exercise choice must be strengthened. Information collectors must provide explicit and succinct privacy policies and user agreements. It is imperative to guarantee that data subjects possess clearly delineated rights to be informed about and to choose the utilization of their personal information.

Table 1. Rights of personal information subjects and corresponding obligations of processors[1].

Subject Rights of Personal Information	Obligations of the Processor
Right to Be Informed (Right to Know Necessary Information, Right to Request Explanation)	Obligation to Inform and Explain
Right to Decide (Right to Consent to Processing, Right to Refuse Processing, Right to Limit Processing, Right to Withdraw Consent)	Obligation to Obtain Consent, Obligation to Provide Natural Options in Algorithmic Decision-Making, Obligation to Delete
Right to Access and Copy	Obligation to Provide Personal Information or Copies of Personal Information
Right to Data Portability	Obligation to Facilitate Data Transfer
Right to Rectification; Right to Supplement; Right to Deletion	Obligation to Rectify; Obligation to Supplement; Obligation to Delete and Cease Processing
Right to Necessary Protection of Personal Information	Obligation to Ensure Security
Right of Close Relatives to Access, Copy, Rectify, and Delete the Personal Information of Deceased Individuals for Their Own Interests.	Obligation to Provide Personal Information; Obligation to Rectify and Delete; Obligation to Cease Processing

[1]Source: Standing Committee of the National People's Congress. (2021). Personal Information P rotection Law. 1 November 2021. Retrieved from https://fund.pingan.com/nasfile/1676251443139. pdf

China should also establish a comprehensive administrative penalty system to impose punishments for unlawful activities, including fines and the termination of company licenses, therefore establishing an effective deterrence and punitive framework (Cheng, 2023). On top of that, the means of redress for data subjects to exercise their rights should be improved. Efficient mechanisms for complaints and appeals must be developed to facilitate data subjects in initiating litigation or seeking redress. The methods and procedures for claiming personal information rights have to be streamlined to reduce complexity and associated costs. A robust complaint and reporting system must be established to enable data subjects to effortlessly report breaches of their personal information to appropriate authorities and get prompt replies and remedies. Moreover, it is essential to augment public education and awareness

campaigns. These initiatives should seek to enhance the awareness and advocacy of data subjects. This approach may motivate people to actively safeguard their personal information.

In conclusion, by thoroughly addressing infringement through legal avenues—such as refining legislation to furnish victims with a legal foundation, intensifying penalties for violators, and streamlining access to legal recourse—we can significantly bolster the initiative of data subjects to assert their rights and guarantee optimal protection.

5.2. Defining the legal boundaries of personal information rights

Clear legal restrictions and policy guidelines must be created to delineate the bounds of personal information rights, balancing these rights with other societal objectives. First, legislation need to delineate the parameters and constraints of personal information rights. The legislation must delineate the parameters of personal privacy, as well as stipulate the conditions for the collection, use, storage, transfer, and disclosure of personal information. It must delineate legal obligations for personal information in certain sectors, like healthcare, banking, and education.

Secondly, actions must be directed by the principles of genuine intent and consent. The acquisition and use of personal information must possess a legitimate and rational purpose and need the express agreement of the data subject. Legislation must establish unequivocal principles of purpose and permission, mandating data processors to notify data subjects about the use of their information and get their voluntary consent. Furthermore, more stringent restrictions must to be enforced regarding the gathering and use of sensitive personal information.

Thirdly, a balance must be struck between individual rights and the general interest. Defining the parameters of personal information rights necessitates a balance between the right to privacy and considerations of public interest, national security, and criminal investigations. The legislation shall delineate the instances and conditions under which personal information rights may be justifiably curtailed to prioritize public interest, national security, or other legitimate concerns. Some scholars believe it is necessary to reconsider legal principles, especially the principles of openness and personal data protection, and suggest adopting an alternative solution of "anonymization" to balance transparency and personal data protection (Guerrero, 2020).

Fourth, Data subjects must own significant authority over their personal information, including the rights to access, amend, delete, limit, or retract their personal information at any time. Data processors shall respect the preferences of data subjects and provide accessible tools for them to assert their rights.

Last but not least, regulatory and accountability frameworks must be enhanced. Robust regulatory authorities and accountability frameworks must be created to oversee and sanction violations of personal information protection legislation. Regulatory authorities must possess sufficient enforcement powers, perform frequent inspections and evaluations, monitor compliance among data processors, and impose suitable fines on offenders.

5.3. Proactive explorations to alleviate the burden of proof

To alleviate the burden of proof for personal information rights holders, the aggrieved party can provide preliminary evidence on the elements constituting personal information infringement. Judges first formulate a provisional ruling upon receiving preliminary evidence from the aggrieved party. Subsequently, the information processor is had the chance to provide counter-evidence. This series of events culminates in the judge rendering a final ruling. Consequently, the preliminary burden of evidence for the rights holder is significantly reduced; they need simply persuade the court of the occurrence of personal information violation. If it can be shown that there is a significant likelihood that the collective management of personal information led to a breach, then a causal link establishing culpability is successfully established (**Table 2**). This proof method is similar to the requirement in autonomous driving infringement in that the infringed party only needs to provide preliminary evidence to prove the causal relationship between the defect and the damage (Chen and Cai, 2024).

Table 2. Burden of proof between the subject of personal information and the information processor.

Burden of Proof for the Subject of Personal Information:	**Burden of Proof for the Information Processor:**
Existence of Personal Information Processing Activities Infringement of Personal Information Rights by the Processing Activities Resulting Damage	1. Absence of Fault (Fulfillment of Information Security Protection Obligations)
Causal Relationship Between the Processing Activities and the Infringement of Rights (Causation Required for Establishing Liability) Causal Relationship Between the Infringement of Personal Information Rights and the Damage (Causation Related to the Scope of Liability)	2. Lack of Causal Relationship Between the Damage and the Information Processing Activities

Additionally, the property aspect of personal information rights should be emphasized. When holders of personal information rights have difficulties in substantiating their losses, ascertaining the compensation amount becomes intricate. In such instances, compensation may be determined by either the losses incurred by the person or the advantages obtained by the information processors. This method guarantees equitable recompense that corresponds to the repercussions of the data breach. In cases when losses and benefits are difficult to measure, the court may use discretion to ascertain the compensation amount or implement a statutory minimum compensation provision (Wang, 2024). Furthermore, in instances of intentional infringement, the use of punitive penalties is advised to discourage such improper conduct by elevating the financial repercussions of infringement.

In situations where personal information is disseminated across many organizations, data processors must demonstrate that they have established robust safeguards to protect people' personal information. Data processors may preserve and provide documentation, including operation logs, audit records, and permission forms, as proof. These documents evidence adherence to legal obligations and confirm that suitable technological and organizational measures have been implemented to safeguard personal information. Furthermore, based on frameworks established by the European Union's General Data Protection Regulation (GDPR), data controllers or

processors may be obligated to prove that they have implemented "appropriate technical and organizational measures" (GDPR, Article 24, 40).

5.4. Strengthening judicial coordination in personal information protection

Enhancing the criminal and civil coordination mechanisms for judicial protection of personal information can be approached from several angles. Firstly, promoting legislative coordination and alignment. Bridging and coordinating different legal domains is crucial for the protection of personal information. Relevant legislation should be interconnected to avoid conflicts and gaps in legal provisions. Legislative bodies should regularly review and amend relevant laws to ensure that criminal and civil provisions complement and align with each other seamlessly. Legally, comprehensive regulations must be instituted to elucidate the cooperation processes between criminal and civil authorities in safeguarding personal information. Legislation must clearly delineate the criteria for identifying personal information violations, the nexus between criminal culpability and civil restitution, together with the relevant court processes and evidentiary standards (Shi and Li, 2023).

Secondly, enhancing collaborative procedures among law enforcement agencies. Judicial authorities and law enforcement agencies must develop more robust collaborative procedures to enhance the integration of criminal and civil dimensions in safeguarding personal information. In judicial practice, legislators should develop tailored regulations based on standards such as the nature of information, the degree of information processing, and the elements of harm (Cui and Qi, 2021).

This involves improving collaboration in information exchange, case referrals, and collaborative investigations to guarantee that violations are handled and prosecuted efficiently and promptly.

Thirdly, improving the professional proficiency of judicial staff. Enhancing training and education for court officials is crucial to augment their competence and decision-making regarding personal information protection. Judicial professionals must possess a comprehensive grasp of both criminal and civil law. They must be able to precisely detect the type of personal information violations. According to their evaluations, they must also be capable of initiating the appropriate criminal or civil legal processes to rectify these violations.

Fourthly, enhancing the collecting and preservation of evidence. Cases involving the protection of personal information often include intricate evidence collecting and preservation efforts. Improving the acquisition and safeguarding of evidence in instances of personal information breaches is essential. This guarantees the integrity and reliability of the evidence. Thus, this reinforces the foundation for both criminal and civil legal proceedings. In addition, some scholars believe that using technological means such as algorithm compliance and algorithm supervision can strengthen the protection of sensitive personal information (Li and Jiang, 2023).

Moreover, supporting public interest litigation in civil matters (Zhang, 2024). Civil public interest litigation is a principal mechanism for promoting the protection of personal information. Individuals and groups need motivation and assistance to initiate civil public interest litigation. These litigations seek to rectify violations of

personal information. Offering this assistance provides victims more avenues and strategies to safeguard their legal rights. Scholars advocate for the active participation of all parties in personal information protection (Tan and Wei, 2022).

Last, enhancing compensation systems. In orchestrating criminal and civil responses to personal information protection, it is essential to develop the compensation processes to guarantee that victims get prompt and effective restitution. Establishing a dedicated fund for personal information protection to recompense victims for their losses and promote punitive punishments for violations should be considered.

To safeguard personal information efficiently, it is essential to improve the collaboration between criminal and civil systems. This entails harmonizing laws, enhancing interaction and agreements between criminal and civil authorities, escalating the costs and severity of punishments, strengthening relief procedures, and augmenting public awareness and education (Yang and Shi, 2023). Consequently, a cohesive and well-integrated system may be built. This approach would more efficiently protect the security and privacy of personal information while maintaining the validity and integrity of personal information rights.

6. Conclusion

Judicial remedy is the primary mechanism for safeguarding personal information rights and acts as the last bastion for maintaining equity and justice. In the digital economy, the court system must unequivocally fulfill its responsibility in advancing personal information protection. It is essential to precisely delineate the parameters of personal information rights, enhancing court regulations, and proactively investigate alternatives to mitigate evidentiary issues. Furthermore, enhancements are necessary for the public interest litigation framework for personal information protection. Improving coordination with prosecutorial entities, consumer protection agencies, and cyber administration departments is essential. In addition, it is essential to establish and improve systems that unify and synchronize civil and criminal safeguards for personal data. These efforts may proficiently tackle the concerns and obstacles encountered in the judicial safeguarding of personal information. They facilitate the effective management of the link between personal information protection and the development of the digital economy. Ultimately, these initiatives will foster legal and sustainable development within the digital economy.

This article has certain limitations in terms of research scope and data collection. The article discusses the limitations and future paths of personal information protection based on China’s legal framework and judicial practice. However, due to differences in legal systems and judicial practices among different countries and regions, the conclusions drawn in the article may not fully apply to other countries or regions. Due to time and resource limitations, this study could not extensively collect all the latest research findings and cases on the judicial protection of personal information domestically and internationally. Therefore, the discussion on certain aspects may need to be more comprehensive.

Future research can further expand to cross-border comparisons, analyzing the legal frameworks, judicial practices, and successful cases of personal information

protection in different countries and regions to provide a more comprehensive international perspective. With the development of big data and artificial intelligence technology, future research can more efficiently collect and analyze the latest research results and cases on personal information judicial protection at home and abroad to provide more comprehensive data support.

Author contributions: Conceptualization, ZC and QC; methodology, ZC; validation, QC; formal analysis, ZC and RG; investigation, ZC and RG; resources, ZC and QC; data curation, ZC, RG, ZJ and HW; writing—original draft preparation, ZC and FH; writing—review and editing, QC, RG, ZJ and HW; visualization, RG; supervision, QC; project administration, QC and FH; funding acquisition, QC. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The National Social Science Fund Youth Project of China, grant number [22CFX018], and China Scholarship Council (CSC) programme, grant number [202206270151].

Conflict of interest: The authors declare no conflict of interest.

References

Boerman, SC, Kruikemeier, Borgesius, FJZ,2021. Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data. communication research.48(07).953-977.

Chen, Z.; Cai, Q.; Wei, H,2024. Distribution of the Burden of Proof in Autonomous Driving Tort Cases: Implications of the German Legislation for China. World Electr.Veh. J. 2024, 15, 305. https://doi.org/10.3390/wevj15070305.

Cheng, K, 2023. The Implementation Basis and Institutional Logic of Administrative Penalties in Personal Information Protection. Law Science. 11, 57-72.

Cheng, X, 2023. On the Rights and Interests of Personal Information. Journal of the East China University of Politics & Law. 26(01), 6-21.

Cui, SJ, Qi, P,2021. The legal construction of personal information protection and privacy under the Chinese Civil Code, Computer Law & Security Review. 41,105560. DOI10.1016/j.clsr.2021.105560.

Guerrero, BG,2020. Protection of personal data in the judiciary: A new look at the principle of publicity of judicial. Revista Chilena De Derecho Y Tecnología. 9(02). 33-56, DOI:10.5354/0719-2584.2020.54372.

Kong. X, 2022. On the Administrative Regulatory Path for Personal Information Protection. Administrative Law Review. 1.

Legal Compliance Department Research Group of China Eastern Airlines Corporation Limited, 2021. The Burden of Proof in Judicial Protection of Personal Information. Journal of International Economic Law. 4, 1-9.

Li, D, 2023. On Compensation for Mental Distress Caused by Infringement of Personal Information Rights. Law and Economy. 4, 134-148.

Li, Q, Jiang, T, Fan, XJ. 2023.Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions. information & culture. 58(3) Page247-273. DOI:10.7560/IC58302.

Li, XH, 2020. Information Privacy Protection in the New Chinese Civil Code: Priority or Replacement? Frontiers of Law in China, 15(3),313-338.DOI:10.3868/s050-009-020-0018-7.

Ministry of Industry and Information Technology of the People's Republic of China, Report on Apps Violating Users' Rights (2022 First Batch, Total Batch No. 21)，https://www.miit.gov.cn/jgsj/xgj/APPqhyhqyzxzzxd/tzgg/art/2022/art_5b6fbbf21d8742cbb54125d5ba18ada7.html. 2024.9.5.

People's Daily Online, People's Commentary: Xpeng Motors Fined for Collecting Facial Data, https://baijiahao.baidu.com/s?id=1719262465231955873&wfr=spider&for=pc.2024.9.22.

Personal Information Protection Law of the People's Republic of China, Article 2.

Shanghai Consumers Council, China Consumers Association: Strengthen Algorithm Regulation to Protect Consumer Rights, https://sghexport.shobserver.com/html/baijiahao/2021/01/11/333647.html.2024.9.22.

Shi, J, Li, X, 2023. Dilemmas and Solutions in the Criminal Justice Connection for Infringing Citizens' Personal Information. Jilin University Journal Social Science Edition. 63(05), 78-90+237. DOI: 10.15939/j.jujsse.2023.05.004.

The Chinese Central Government's Official Web, Personal Information Protection Law of the People's Republic of China, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.2024.9.22.

The Supreme People's Procuratorate of the People's Republic of China, Guiding Opinions on Actively and Prudently Expanding the Scope of Public Interest Litigation Cases, Published on 18 September.

Wang, K, 2024. A Study on the Application of Damage Compensation Rules in Civil Public Interest Litigation for Personal Information Protection. Hebei Law Science. 42(07), 50-67. DOI: 10.16494/j.cnki.1002-3933.2024.07.004.

Xu, K, Quan, L, 2024. Theoretical Restatement of Personal Information Rights. Gansu Social Science. 2, 139-150.

Xu, T; Li, W. 2022.Japanese Personal Information Protection System and Its Enlightenment to China. 2022 International Conference on Advanced Enterprise Information System (AEIS). 02-04 December 2022. DOI: 10.1109/AEIS59450.2022.00012.

Xue, W, 2024. The Operational Model, Theoretical Dilemmas, and Protection Pathways of Personal Information in the Era of Big Data. Chinese Journal of Maritime Law. 35(02), 103-112.

Yang, W, Shi, W, 2023. Examination and Adjustment of the Conviction Mechanism for Infringing Citizens' Personal Information Under the Civil-Criminal Connection: A Perspective Embedded with Personal Legal Interests. Shandong Judges Training Institute Journal. 39(02), 33-46. DOI: 10.14020/j.cnki.cn37-1430/d.2023.02.004.

Zhang, Y, 2023. The "Design Protection" of Personal Information in Human-Machine Dialogues: Focusing on the ChatGPT Model. Library Tribune. 5.

Zhang, Z, 2024. The Mechanism of Civil Public Interest Litigation in the Protection of Personal Information. Tribune of Political Science and Law. 1-14. http://kns.cnki.net/kcms/detail/11.5608.D.20240909.1033.004.html.2024.09.022.

Zhou, H, 2021. Parallel or Intersecting: The Relationship Between Personal Information Protection and Privacy Rights. Peking University Law Journal. 5.