MINDWELL SCIENCE PRESS SDN. BHD.

Journal of Emerging Technology Governance
Volume 1, Issue 2

RESEARCH ARTICLE

Adjusting the Rules on Data Circulation and Privacy Protection under the Principle of Proportionality

Yuna Li[1], Hongxuan Wang[1,*]

[1] *School of Law, Xi'an University of Finance and Economics, Xi'an 710100, Shaanxi, China*

* **Corresponding author:** Hongxuan Wang, E-mail: wanghongxuan@mail.xaufe.edu.cn

Published: 28 August 2026

Abstract

Strengthening data circulation and privacy protection is an urgent requirement of building a digital society. Data circulation creates value and adds value, but its dynamic mobility and its value-generating character also frequently give rise to such security problems as the theft, sale and unlawful use of personal privacy data. To ensure the harmonious coexistence of data technology enablement and individual privacy interests, the principle of proportionality needs to be applied in depth in practice: to seek the logic of adjustment between data circulation and privacy protection along the theoretical and value dimensions, and to construct a rule of appropriateness, a rule of necessity and a rule of balancing, forming a path of adjustment in which the three rules advance level by level and the levels are complete.

Keywords: principle of proportionality, data circulation, privacy protection, rule adjustment

1 Introduction

The promulgation of the *Personal Information Protection Law of the People's Republic of China* (hereinafter the *Personal Information Protection Law*) has supplied a legal basis and an institutional guarantee for privacy protection, but privacy protection in different fields still requires the relevant rules to be refined. The *Personal Information Protection Law*, for example, provides in its general provisions only the general principles governing the processing of personal information by state organs, and makes no specific provision for privacy protection in the field of data circulation. Articles 21 to 26 of the *Data Security Law of the People's Republic of China* (hereinafter the *Data Security Law*), by contrast, supply a basic legal framework for such problems in the field of data circulation as classified and graded data protection and the administration of cross-border data flows, but lack any content on privacy protection. The different emphases of the two statutes may therefore give rise to duplicate protection or to insufficient protection in the course of implementation, which to a certain extent affects the effectiveness of data privacy protection.

In order to balance the multiple subjects and multiple interests involved in data privacy[1], and proceeding from comparative law, Wang Xixin, Peng Chun and others advocate a "proportional balance", requiring that data-processing activities conform to statutory conditions and to the principle of proportionality[2]; Mei Xiaying advocates a "risk balance", matching control measures over data reasonably to the magnitude of social risk and releasing the vitality of data[3]; Ding Xiaodong represents a "contextual balance", understanding privacy interests in context and promoting the circulation of private information within concrete contexts[4]; and Liu Deliang supports a "market balance", recognising the individual's private property right over his information and safeguarding the equilibrium of supply and demand in the market for personal information transactions. Of these, data privacy interests cannot be classified simply as property rights, so the market-balance mechanism does not apply; business contexts differ in standard and their boundaries are blurred, and the contexts in which data are used change dynamically, so the contextual-balance mechanism does not apply; and privacy protection finds it hard to identify a clear "focus" of risk, risk factors are hard to quantify, the anonymised information provided for in Article 4 of the *Personal Information Protection Law* is not protected by law, and "de-identification" is treated in Article 51 merely as a security measure, so the risk-balance mechanism is likewise hard to apply.

It is precisely because of these obstacles that the significance of the principle of proportionality becomes all the clearer. Beginning with the first case in which the principle of proportionality was applied, the *HSBC case* of 1999, the principle has been progressively absorbed by academic circles and by practice by reason of its high degree of operability, and Article 13 of the *Personal Information Protection Law* is a concentrated expression of it. Surveying the current state of privacy protection under data circulation, rule adjustment may be achieved through the following steps: first, is the purpose pursued

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

by the data-processing subject legitimate, and by what standard is that purpose to be reviewed? Second, is there an effective means of achieving the objective equally well that restricts individual rights and interests less? Third, are individual and public interests in balance, and has an excessive burden been placed on individual interests?

2 A Jurisprudential Reflection: An Analysis of the Conflict between Data Circulation and Privacy Protection

2.1 The Manifestation of the Conflict

The data relevant to privacy protection may be divided into two categories: personal information and personal data. Personal information is information of every kind, recorded by electronic or other means, that is connected with a natural person who is identified or identifiable; personal data, by contrast, is the record of personal information presented by electronic or other means[5]. Data privacy, situated in the field where the two overlap, denotes the right of protection an individual or organisation enjoys in respect of certain information that ought not to be made public in the course of data processing. The economic information, social media activity and other content it covers is highly likely to become the data foundation for the future development of affective computing technology[6], and the data subject will confront problems of more dimensions, including infringement of personal privacy and restriction of the rights to freedom and equality[7]. At the same time the security risk of data privacy has risen to the national level: once data privacy crosses borders without effective control, other states may conduct intelligence collection and analytical assessment in a targeted way, bringing a potential and incalculably grave threat to national security.

(1) Improper handling of privacy in the data trading market. Data privacy includes but is not limited to identity information, location information, financial circumstances, consumption data and personal relationships. Some go further, using background programs to record sound and image and inducing users to authorise permissions by means of vague privacy clauses[8]. Once such data are improperly traded, it is very easy for the party acquiring the data to construct an accurate user profile and thereupon carry out targeted manipulation. The online résumé trafficking case exposed by a reporter of *China Youth Daily* in a 2019 undercover investigation is an example. Privacy is a symbol of personal dignity and should not be given any tradable value carrying a property attribute[9]. This not only infringes the individual's right to privacy but deals a severe blow to the trust system of society.

(2) The crisis of privacy disclosure in public data sharing. Data sharing aims to eliminate information islands and to promote the maximally valuable use of data storage, use and exchange[10]. The interconnection and interoperability of data sharing aggravate the crisis of privacy disclosure. Data circulation brings humanity unprecedented convenience while also forming "an alien force independent of humanity"[11]; privacy protection, an issue traditionally confined to physical space, has now extended into virtual space, forcing people to re-examine and reshape the principles and strategies of privacy protection.

2.2 Tracing the Causes of the Conflict

(1) Data property rights are unclear. Barzel observed in *Economic Analysis of Property Rights* that the precondition for defining property rights is that the owner of the asset and potential competitors alike have a clear cognition of that asset and a deep understanding of the intrinsic attributes by which it creates value[12]. The definition of property rights is thus affected by the attributes of data. Visualised data, for example, occupy a dominant position in the definition of property rights by reason of their intuitiveness and their directly applicable value; structured data come next, requiring a certain amount of processing but possessing clear value; and metadata, which cannot directly create value, occupy a weak position in the definition of property rights by reason of their abstractness and breadth. This means that not every data resource can have its property rights defined directly and economically, and where the cost of definition far exceeds the potential benefit, an ambiguous treatment of property rights becomes a reasonable choice. Moreover, the definition of property rights over private data, public-sector data, industrial and commercial enterprise data and other privacy data differs according to their distinctive claims of interest.

(2) Supervision of data circulation is absent. Government supervision is crucial in the field of data circulation and needs to cover comprehensively such dimensions as the security of data operations, technological innovation and platform compliance. Data circulation, as the key pathway for releasing the potential of data, bears directly on the realisation of data value. Excessive government supervision may affect the efficiency of data circulation, while insufficient supervision may give rise to risk. Finding and maintaining this delicate balance has therefore become a major difficulty in formulating a supervisory strategy. Judged by the *Cybersecurity Law* and the *Personal Information Protection Law*, the current problems of government supervision over data circulation appear mainly in imperfect legislation, an unsound system of prior and concurrent supervision, and a low entry threshold. At the same time, in the course of the circulation and use of data, the

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

government's follow-up monitoring is not timely, so that its system of security precautions is unsound.

(3) Relief for privacy protection is lacking. In the field of data circulation the scope of the definition of data privacy harm and the standard of compensation for damage are not yet clearly provided for in law. Judicial organs also frequently dismiss claims on the ground that the plaintiff cannot prove his damage. Data privacy harm cannot be covered by the traditional rules for determining damage, which produces many unjust consequences. First, the individual cannot obtain adequate protection because the data privacy harm is not recognised. Second, because data privacy harm cannot be accurately predicted or quantified, the amount of compensation is extremely low. Finally, relief for this kind of harm is constrained by resources and by legal authorisation and relies too heavily on administrative supervision, which readily forms path dependence and makes the path of relief for data privacy harm impassable.

3 The Logic of Relief: Justifying the Introduction of the Principle of Proportionality

To balance the conflict between data circulation and privacy protection, the principle of proportionality may be introduced to harmonise them. The principle of proportionality is the basic method of weighing interests; it can supplement the protection of private subjects in situations such as this, where public and private legal interests coexist, balance interested parties that differ in strength, and explore the optimal path of harmonisation[13].

3.1 Deconstructing the Content of the Principle of Proportionality

The adjustment of data circulation and privacy protection is in substance a weighing of multiple interests, and the principle of proportionality is precisely the legal instrument that can concretise an abstract weighing of interests into a normative structure and thereby allocate resources justly. Following the framework of the principle of proportionality widely adopted in the field of administrative law, it may be refined into three sub-principles: appropriateness, necessity and balancing, which together constitute the essence of the principle.

(1) The principle of appropriateness. This is the initial stage in applying the principle of proportionality. It judges mainly whether the purpose is legitimate, requiring that the measure adopted be appropriate and at least conducive to realising the established objective of interest. It resembles the requirement of Article 6 of the *Personal Information Protection Law* that "the processing of personal information shall have a clear and reasonable purpose and shall be directly related to the purpose of processing". The installation of surveillance equipment in a public place, for example, has as its original intent the maintenance of public security and the strengthening of management, but the purpose of this act must be strictly limited, and it is prohibited to misuse the personal information collected in other unauthorised fields. Consideration under the principle of appropriateness must also be placed within a specific context, ensuring that the purpose is pure, and the key to judging the legitimacy of a purpose lies in what interest it is meant to realise.

(2) The principle of necessity, also known as the principle of least infringement, has at its core the optimisation of means in the course of realising a purpose. That is, among the several pathways by which the same objective might be achieved, priority should be given to the scheme that causes the least interference with the interest restricted. Such expressions in the *Personal Information Protection Law* as "reasonable scope", "minimum scope" and "minimum manner" are practical glosses on the principle of necessity. Collecting personal information within the minimum scope embodies a cautious attitude towards the exercise of public power.

(3) The principle of balancing, also called "the principle of proportionality in the narrow sense", has at its core the search for a balance between restriction and protection. That is, at the moment of strategic choice, the purpose of the action and the consequences it may give rise to must be weighed comprehensively, ensuring that the interest obtained in achieving the objective manifestly exceeds the harm thereby caused[14]. Take privacy protection: if extreme measures were adopted and the collection of any personal information were prohibited outright, the risk of data privacy disclosure would indeed be effectively contained, but the development of the digital economy would undoubtedly be dealt a heavy blow, and the realisation of individuals' basic rights to life would even be indirectly obstructed. This plainly does not conform to the principle of balancing.

The review framework of the principle of proportionality is shown in Table 1.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Table 1 Review framework of the principle of proportionality

Level	Sub-principle	Object of review	Review criterion
First level	—	Data circulation and public interest vs. data privacy protection and private interest	The principles of lawful, legitimate and necessary processing of personal privacy information, without excess
Second level	Principle of appropriateness	The initial purpose and the true purpose of data privacy processing	—
	Principle of necessity	The means of processing data privacy and risk assessment	—
	Principle of balancing	Public interest, private interest, the harm suffered and the cost of processing	—

3.2 The Logic of Adjustment under the Principle of Proportionality

(1) Delimiting the boundary of public authority's intervention in data circulation. The principle of proportionality has extended from a principle of public law to a criterion for defining individual rights, and possesses the theoretical significance of examining whether public power's restriction of private rights is legitimate. Where individual rights can be restricted and in fact are restricted, the intervention of the principle of proportionality is necessary[15]. Chapter VI of the *Personal Information Protection Law* sets clear boundaries of power and principles of performance for administrative organs, prevents the excessive collection and use of personal information, and emphasises the proportionality of data circulation. The principle of proportionality, oriented towards the balance of legal interests, delimits the boundary of the intervention of public power and supplies practicable and reasonable protection for data privacy.

(2) Correcting the imbalance between the security and the exploitation of data. The rule of "processing within a reasonable scope" in the *Personal Information Protection Law* confers interests on the information processor while restricting the individual's privacy interests. In the digital age the equal status of the traditional civil subject is changing. When an application notifies a user of a permission to obtain identity information, for example, the user is often caught in the helpless choice of "consent or abandon": refusal means the software cannot be used, and privacy protection is eroded under the dominance of a platform monopoly. In such a situation the principle of proportionality can both regulate conduct in which a private subject occupies a position similar to that of a public authority, making that conduct conform to private-law autonomy, without losing the constraint of public law. The principle of proportionality can construct for the judging subject a paradigm of reasoning that is both operable and verifiable, and can supply the grounds of argument for the final conclusion.

4 Rule Adjustment: The Relief Path of the Principle of Proportionality

The relief path of the principle of proportionality comprises three levels: first, that the purpose of a government's or enterprise's processing of privacy data is legitimate and that a causal relation exists between means and purpose; second, that the government or enterprise chooses the means that has the least effect on privacy protection in order to achieve that purpose; and third, that the public interest enhanced by the conduct of the government or enterprise is proportionate to the privacy interest it damages.

4.1 Appropriateness: Reviewing the Legitimacy of the Processing Purpose

1. Active review of public-interest purposes in "statutory processing". Clarifying the true purpose of processing is the precondition for constructing a standard of legitimacy review. Under Articles 13 and 35 of the *Personal Information Protection Law*, where a state organ processes personal information in the performance of its statutory duties or statutory obligations, it need not obtain the individual's consent and possesses a basis of legality[16]. Such processing is in substance a reasonable restriction of privacy interests by law on consideration of the public interest, its core being service to public-interest objectives. It is worth noting that statutory processing dispenses with the ordinary requirement of notification and consent, but where in a particular case a purpose was notified, the true purpose actually governing the processing conduct should be analysed in depth.

In statutory processing an active standard of purpose-legitimacy review is adopted, strictly verifying whether the true purpose of processing conforms to the provisions of statutes and administrative regulations, and this derives from the constraint of the principle of legal reservation. In restricting data privacy the processing subject should actively follow the clear guidance of laws and regulations, ensuring the legality and legitimacy of the privacy processing. Conversely, if the basis for processing is confined to administrative rules or to normative documents of a lower level, the purpose of processing may be regarded as improper for want of adequate legal authorisation. Establishing an active review benchmark

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

supplies the basis of right for privacy protection and restrains conduct that, under the guise of the public interest, improperly restricts the right to data privacy.

2. Passive review of private-interest purposes in "authorised processing". In view of the vagueness of the initially notified purpose, focus must fall on identifying the private-interest purpose that truly governs and determines the direction of personal privacy information. Faced with the strategies processors may adopt in practice, such as concealing the true purpose or layering multiple purposes, a plurality of review methods should be adopted. Positive inference, for example, analyses in depth the processing purpose the processor expressly notified and exposes any true purpose that may lie behind it, distinguishing the dominant from the accessory purpose; negative inference, by contrast, takes the processor's concrete conduct and verifies in reverse which processing purpose the measures adopted are consistent with, thereby fixing the true purpose. The substance of the processing purpose must be grasped precisely, so as to avoid substantive inequality between the processor and the privacy subject and to prevent the subject's consent from becoming a mere formality[17].

In authorised processing a passive standard of purpose-legitimacy review is adopted, that is, the review focuses on whether the processor's conduct is prohibited by law. This standard is established in order to balance the delicate relationship between privacy protection and exploitation: it respects the autonomy of the civil subject while opening space for commercial exploitation. In concrete operation, although it is not required that every act of authorising privacy obtain direct authorisation from statutes or regulations, the reviewer must ensure that the processing conduct does not contravene any prohibitive provision of law. In commercial services predicting a natural person's genetic information, for example, reference should be made to the *Biosecurity Law* and the *Regulations on the Administration of Human Genetic Resources*, and the review of the processing purpose should proceed with the utmost caution. Establishing only a benchmark of passive purpose review in such processing is not enough to constitute a refined screening mechanism; rather, processing that meets the requirement of legitimacy should be brought into review as far as possible, laying the foundation for the subsequent review of rules.

4.2 Necessity: Typological Restrictions on the Means of Processing

The *Data Security Law* establishes a system of classified and graded data protection, which is of far-reaching significance for reconciling the contradiction between data circulation and privacy protection. Yet data privacy has complex attributes and manifold forms of expression: by what means, then, are the degrees of necessity for different processing subjects, different processing conduct and different types of information processed to be distinguished?

1. Risk assessment of the means of processing. Establishing the principle of necessity can guide the processor of privacy data to employ appropriate means, reaping the benefit that information processing brings while averting the loss it generates. In necessity review, risk assessment is the key factor affecting the connection between purpose and means, and the two together determine what degree of necessity should be reached in adopting a means of processing.

The risk assessment of data privacy may proceed around the consequences of processing. First, the nature of the personal information. The *Personal Information Protection Law* divides personal information into sensitive information and general information; sensitive information frequently involves data privacy, and the risk confronting the processing of sensitive information is greater than that confronting the processing of general information. Second, the basis and purpose of processing. Ordinarily, statutory processing proceeds from the public interest and in strict accordance with legal procedure in an orderly way, and the risk it carries is relatively low. An operator, however, may well resort to the authorised processing of personal and private information in order to maximise its economic interest, and the risk carried is greater. Third, comprehensive consideration and ranking. Once sorted, four risk situations emerge, in the following order: authorised processing of sensitive information, statutory processing of sensitive information, authorised processing of general information, and statutory processing of general information[18]. A review standard built on this typological basis can supply judicial guidance in which market subjects may find the boundary of their conduct made clear.

2. The connection between purpose and means. In the authorised processing of sensitive information the connection between purpose and means must be maximal, so as to prevent the autonomy of the processing subject and to avoid harm to personal privacy information. Concretely, the means must have certainty and inevitability in attaining the purpose; the means of information processing should be entirely consistent with the means presupposed by the processing purpose; and the highest review benchmark is adopted. In the statutory processing of sensitive information and the authorised processing of general information the connection between purpose and means should be ordinary, lower in degree than for the authorised processing of sensitive information; the processor must supply reasonable grounds for the means attaining the purpose, the reviewer must distinguish the connection in the two cases, and a medium review benchmark is adopted, with further determination possible in the light of concrete circumstances and social effects. In the statutory processing of general information the connection between purpose and means need only be minimal: the reviewer may find no reasonable connection only where no ground supports the means attaining the purpose. The requirement of minimal connection helps processing bodies to raise the efficiency of social management and to give full play to the economic utility of personal

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

information. The connection between purpose and means in the processing of personal information is shown in Figure 1.



Figure 1 The connection between purpose and means in the processing of personal information

4.3 Balancing: The Minimal Impairment of Privacy Interests in Data Circulation

The principle of balancing attends more to balancing total cost against benefit. The state may, by refining the supervisory mechanism of data circulation and widening the path of privacy relief, attain a balance between the full circulation of data and the protection of privacy. In addressing the supervision of data circulation, the legislative framework should delimit precisely the duties and instruments of supervisory bodies, may provide for "legal supervision" in a dedicated chapter, and should make systematic arrangements for prior, concurrent and subsequent supervision. In addressing relief for data privacy, the rules of relief should be adjusted in view of the distinctive character of data privacy harm.

1. Refining the supervisory mechanism of data circulation. As for prior supervision, the first step is to construct a certification system for data circulation. As the threshold of market access, every entity engaged in data-circulation services must submit a detailed filing of its data-processing activities to a designated supervisory body and undergo review. Those that pass are granted a data-circulation security certification, which is publicly announced. As for those that do not meet the standard, the supervisory body should order rectification and, where rectification is inadequate, take measures to restrict or prohibit their data-processing business. Second, for large enterprises, multinational enterprises or organisations processing highly sensitive data (such as children's information, personal privacy information, criminal records and high-value financial data), a system of pre-processing impact assessment reports should be introduced. Such entities must submit detailed reports to the supervisory department in advance, and the department is to assess them carefully and generate a processing schedule, implementing differentiated protection measures for information of different risk levels and ensuring the effective implementation of a graded-safeguard strategy. Finally, establishing a prior consultation mechanism to provide professional answers and guidance on questions arising in the course of data processing is also an indispensable element of prior supervision.

As for concurrent supervision, a long-term tracking and reporting mechanism needs to be constructed. Supervisory bodies should periodically review the data-processing activities of the relevant enterprises or organisations, forming a management process of "submission of reports—review and inquiry—public disclosure". Enterprises must submit detailed data-processing reports to the supervisory body quarterly or annually, which not only allows the body to keep abreast of developments but also supplies the basis for a rapid response to potential crises. Once an anomaly occurs in data circulation, the supervisory body can promptly locate the source of the problem and take the necessary measures to minimise the harm.

2. Widening the path of relief for privacy harm. *(1) Statutorification of the determination of data privacy harm.* Within the legal framework of privacy protection, direct harm and subsequent harm should be distinguished and statutorified, the aim being to delimit precisely the category of infringement recognised by tort law and thereby reasonably to avoid the data-processing subject's bearing of "unbounded liability" for potential unknown risk. This not only ensures the clarity of legal application but also enhances legal foreseeability. At the same time, statutorifying particular types of privacy harm directly simplifies the legal process of establishing causation in tort cases, responds effectively to the "high cost" and

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

"difficulty of proof" that commonly afflict the relief of privacy infringement, and promotes the efficiency of justice.

(2) Optimising the compensation system for data privacy harm. In view of the distinctive character of data privacy, the compensation mechanism should not be confined to a single model of pecuniary compensation but should explore pluralistic paths of relief. Concretely, for reputational harm arising from the tampering of privacy data, a mechanism of reputational restoration should be constructed in addition to economic compensation, ensuring that the measures of relief match the actual assessment of the harm and achieving comprehensive and effective repair of the damage.

(3) Introducing a model of compensation for data privacy harm. At the initial stage a comprehensive model of compensation may be adopted, without deliberately distinguishing pecuniary from non-pecuniary harm, permitting the victim to make a "package" claim and determining a unified amount of compensation after comprehensive consideration of the consequences of the harm. As practice deepens and the law is refined, it is suggested that the compensation model be refined at a later stage through dedicated legislation—borrowing, for instance, from the practice of the United States and setting clear compensation standards or a schedule of tariffs for privacy harm, so that the uncertain factors in the assessment of harm can be converted into concrete results of relief through a clear and operable model, further enhancing the operability and fairness of the legal system.

5 Conclusion

The enactment of the *Personal Information Protection Law* elevates the right to privacy into a new type of interest urgently requiring protection. Data circulation is an important factor in economic and social development in the digital age, and a merely general management or formal review of it poses a great threat to privacy protection. Privacy protection must be combined with the characteristics of data themselves, constructing concrete measures of privacy protection and substantive standards of review. The principle of proportionality, as the first principle of public law, supplies a complete three-stage standard of review for privacy protection from the three levels of purpose, means and the balance of interests, and provides a methodology for balancing the circulation of big data against the protection of privacy interests. It should become the trend of the future.

References

[1] Xu K. The principle of good faith: a trust path to balancing the protection and use of personal information[J]. *Peking University Law Journal*, 2022, 34(5): 1143-1162. [in Chinese]

[2] Wang X X, Peng C. The constitutional foundations of the legal system for personal information protection[J]. *Tsinghua University Law Journal*, 2021, 15(3): 6-24. [in Chinese]

[3] Mei X Y. Social risk control or individual interest protection: two dimensions for understanding the Personal Information Protection Law[J]. *Global Law Review*, 2022, 44(1): 5-20. [in Chinese]

[4] Ding X D. On the intellectual origins and basic principles of the legal protection of personal information: an analysis based on "fair information practices"[J]. *Modern Law Science*, 2019, 41(3): 96-110. [in Chinese]

[5] Miao Z Y. Research on the protection of personal information against the background of building a data trading market[J]. *Tribune of Political Science and Law*, 2022, 40(6): 55-65. [in Chinese]

[6] Wang L S. The application predicament of affective computing and its legal regulation[J]. *Social Science Digest*, 2021(9): 67-69. [in Chinese]

[7] Ma C S. "Fourth-generation human rights" in the context of the smart society and their protection[J]. *China Legal Science*, 2019(5): 5-24. [in Chinese]

[8] Zhao J Y. Research on the personal information protection system in big data transactions[J]. *Journal of Shanxi Finance and Tax College*, 2021, 23(3): 48-53. [in Chinese]

[9] Peng C X. How may the fundamental contradiction in the use of data be eliminated: a jurisprudential clarification of privacy, information and data[J]. *Exploration and Free Views*, 2020(2): 79-85, 158-159, 161. [in Chinese]

[10] Guo H Y. *Research on the Development of Civil and Commercial Law in the Course of Contemporary Chinese Social Transformation*[M]. Changchun: Jilin University Press, 2017. [in Chinese]

[11] Wang C. The choice of model for the civil-law protection of personal information[J]. *Social Sciences in China*, 2019(6): 124-146, 207. [in Chinese]

[12] Barzel Y. *Economic Analysis of Property Rights*[M]. Shanghai: Shanghai People's Publishing House, 1997. [in Chinese]

[13] Zhang L L. The principle of proportionality as a method of weighing[J]. *Law and Social Development*, 2022, 28(3): 187-205. [in Chinese]

[14] Liu Q. Controversies over and reflections on the application of the principle of proportionality[J]. *Comparative Law Research*, 2021(5): 172-187. [in Chinese]

[15] Mei Y. The scope and limits of application of the principle of proportionality[J]. *Chinese Journal of Law*, 2020, 42(2): 57-70. [in Chinese]

[16] Cheng X. On the system of reasonable use of personal information in China's Civil Code[J]. *Peking University Law Journal*, 2020, 32(4): 1001-1017. [in Chinese]

[17] Gao F P. The legitimate basis for the use of personal information: the perspective of interests in data[J]. *Comparative Law Research*, 2019(2): 72-85. [in Chinese]

[18] Wang L J. Constructing the system of review benchmarks for the principle of proportionality in the processing of personal information[J]. *Law Science*, 2022(4): 49-63. [in Chinese]

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.