MINDWELL SCIENCE PRESS SDN. BHD.

Journal of Emerging Technology Governance
Volume 1, Issue 2

RESEARCH ARTICLE

A Collective Approach to Data Governance: The Perspective of Group-Level Data Effects

Qiuru Wang[1,*]

[1] *Zhongnan University of Economics and Law, Legal Master Education Centre, Wuhan 430000, Hubei, China*

*** Corresponding author:** Qiuru Wang, E-mail: wangqiuru@zuel.edu.cn

Published: 28 July 2026

Abstract

The value of data derives from the group characteristics that data present once they have been collected and processed, yet every existing model of data governance emphasises the internalisation of data rights as the individual rights of the data subject. Individualist data-subject rights cannot represent effects at the level of the data group, and group-level data effects ought to be fully taken into account in data governance. Without such consideration data governance cannot genuinely safeguard the social benefit of data, and its effectiveness cannot be brought fully into play. How group-level data effects may properly be incorporated into a model of data governance depends to a greater extent on collective forms of data governance: such collective data-management models as the data trust can offer workable suggestions for establishing a scheme of group data governance. A renewed scheme of group data governance should proceed from three mechanisms—the lawful boundary of data collection, the mechanism of data management, and the mechanism of data use—together with a mechanism of data accountability, so as to achieve a more complete model of data governance.

Keywords: data governance, group effects, relational theory

1 Introduction

Since the entry into the internet era the scale of the digital economy has grown continuously, and it has become an important component of the national economy. The *Global Digital Economy White Paper (2023)* shows that in 2022 the digital economies of five major countries—the United States, China, Germany, Japan and the Republic of Korea—totalled USD 31 trillion, with the digital economy accounting for 58 per cent of GDP, an increase of about 11 percentage points over 2016; the year-on-year percentage growth in the scale of the digital economy was considerable, and the digital economy has continued to drive national development. Shoshana Zuboff proposed informational capitalism, denoting a new mode of production that collects and processes data in order to obtain and accumulate wealth—that is, one that converts data from a readable form of text inside the machine into a resource for production[1]. As Google succeeded in "refining" useless waste data and extracting "behavioural surplus", it shaped a new logic of capital accumulation[2]; more and more enterprises collect users' data in order to make predictions about those users, so that users' behaviour becomes progressively transparent and wealth is accumulated from it. The logic of this is broadly threefold. The first is to sell data directly, although a reckless sale of data readily offends against the law, infringing the rights and interests of the data subject or the interests of a particular group. The second is to use the data collected to act back upon enterprise production. The third is to analyse the data and then predict user behaviour, thereby changing it. A typical example is the Douyin application, which uses its "recommendation" page to display a collection of videos generated by Douyin's dedicated recommendation engine. The value of data derives more from its behavioural influence on network users, and its underlying logic lies in the effect of data on groups. The social-relational theory of data proposed by Salomé Viljoen shows that different data subjects are strongly interrelated, and that this interrelatedness precisely confirms the group-level effects of data. Effects on individuals within a group will indirectly affect the whole group, and the behaviour of individuals within a group will likewise affect the whole group; the data individual will be submerged in the group, so that the interests of the data individual are far less important than those of the data group.

On 19 December 2022 China issued the *Opinions on Building a Data Base System to Better Play the Role of Data Elements* (hereinafter "Data Twenty Articles"), which takes the separation of the three rights as its framework and focuses on four priority directions—data property rights, circulation and transactions, revenue distribution, and security governance—emphasising systematic and comprehensive regulation of the operation of the data economy. Yet whether it be

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.

the domestic model of data governance, which takes "data circulation and transactions" as its core, the model of the United States, which is grounded in "personal information protection", or the model of the European Union, which emphasises prior "informed consent", all internalise data as the rights of the data subject and neglect the group-level effects of data. For this reason it is necessary to set out from the individual-empowerment model of data governance, to examine the failure of the "user empowerment" model and the justification for group-level data effects in data governance, and, proceeding from the model of data collection and the mechanism of data management, to transform the scheme of data governance.

2 A Theoretical Reflection on Data Governance: Group-Level Data Effects

2.1 The Group Effects of Data Governance

Salomé Viljoen proposes a social-relational theory of data governance, advocating that the social relations of data governance be examined along two dimensions, the horizontal and the vertical, from which group-level data effects may be discerned.

1. Horizontal data relations link data subjects. The social relations of data governance unfold around the data subject, the data collector and processor, and the third-party groups that may be affected by the data. The vertical dimension describes the relationship between the data subject and the data collector and processor. At the technical level, the vertical data relation appears as the process by which data pass from the data subject to the data collector and processor; at the legal level it appears in the various rights conferred on the data subject, the various obligations imposed on the data collector and processor, and the allocation of data rights and obligations between the two parties by the relevant law. In fact, the vertical data relation has long been a focus of scholarly research. The vertical relation requires that the relationship of interests between the data subject and the data collector and processor be balanced by allocating rights and obligations between the two parties.

The horizontal dimension describes the interrelatedness between data subjects who are otherwise unconnected, and the interrelatedness between different subjects that share the same group characteristics. At the technical level, the horizontal relation holds that the data subject be parsed through group characteristics and thereby fed back to other subjects. This technical method depicts the outward appearance and inner preferences of the data subject by means of a digital profile, classifying and defining the data subject[3], and then identifies the social-level performance of different data subjects within group characteristics that "contain common fields capable of connecting different datasets"[4-6]. Further, an analysis of group characteristics cannot be carried out among a mere handful of individuals; it must be carried out among a certain number of individuals—that is, among a group. The data interest is at this point generalised into a group interest, and the source of the data is then naturally no longer important: what plays the substantive role is the conclusion drawn from parsing the data and the effect of that conclusion. Throughout the data economy market there are countless examples of several individuals being linked through horizontal relations.

2. The aggregation of data subjects produces group-level data effects. On the basis of relational theory the effect of data collection and analysis on groups may be discerned. Research has shown that group data may be used to develop models, and that models can predict a subject's behaviour and thereby change it, securing market advantage and surplus value[7]. The precondition for developing a model is to treat the data subject as a member of a group rather than as a separate individual; the insight of the group is the foundation on which the model is built, and in this process the data subject is integrated into the group, and the concrete behavioural patterns of the group are extracted through the data subject[8]. In this process the effect on data gradually becomes apparent.

First, the identifiability of data progressively declines. The data collector and processor anonymises and abstracts the personal data of the data subject so that they no longer possess identifiability and can no longer be directly connected with a particular data subject, while at the same time giving rise to group analysis and to decisions made on the basis of that analysis which affect countless data subjects. Anonymised, non-identifiable data also suppress the individual's opportunity to express an objection to his or her own bias within the group or to access the data-processing mechanism. The classifications the data collector and processor makes in analysing the data, and the decisions taken on that basis with respect to a particular group, do not permit the participation of the data subject (the group member), and at the same time sever the data subject's avenue for refusing data analysis.

Second, the effect on the data individual continuously expands. The behaviour of any one individual within a group may affect other individuals, and the range of data risk continuously widens. A data collector may, on the basis of the behaviour of one member of a group, determine new information about other subjects[9]. This mechanism of classificatory prediction operates on the premise of predicting a large number of variables; through its knowledge of the group, the data redefines the group members, and that knowledge of the group arises from countless data subjects, who, when they surrender their own data, are not clear what effect their data may have on the group and on themselves.

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.

Third, the risk of data discrimination grows steadily more severe. Anonymised data collection, classification and prediction are a "shield" for enterprises in mining and analysing data. Research has pointed out that "legal and de facto immunities increasingly benefit private economic power, heightening the vulnerability of ordinary citizens to manipulation, exploitation or political disenfranchisement, and may cause profound collective harm"[2]. Although data-analytic algorithms have always been judged neutral and objective, the social values on which algorithmic intervention in group behaviour rests are those that occupy a dominant position, not objective criteria of interpretation. "The method of maximising objectivism cannot discover values, interests, discursive resources or the way in which organisational knowledge is produced"[10]; so-called scientific objectivity is nothing but "an illusion", and neutrality nothing but "an illusory goal"[11]. However algorithms may be proclaimed neutral and value-free, they may still give rise to improper social discrimination.

2.2 The Justification for Incorporating Group-Level Data Effects into the Model of Data Governance

The basic path of "user empowerment" confers on the data subject the right of data self-determination and imposes a series of obligations on internet platform enterprises in order to regulate their conduct. A model of data protection grounded in the individual does not take the group interest in data into account; attention to the interests of the data subject is of course important, but the protection of the data subject cannot release data processing from other social costs and factors. When a model of data governance is considered and formulated in a comprehensive way, group-level data effects therefore need to be attended to.

1. The absence of group-level data effects leads to the failure of data governance. In particular processes of data collection and processing the interests of the data subject and of the data collector are seriously imbalanced: the data collector holds most of the benefit arising after processing, which in turn stimulates the data collector to collect more data more actively. The absence of any consideration of group-level data effects means that the group interest cannot be represented, and may at the same time cause the incentive mechanism of the data collector and processor to fail. First, group-level data effects cause the mechanism of data collection premised on "consent–informed" to fail, so that the potential risks arising from the aggregation of group data cannot be prevented. Second, group-level data effects cause social information to become distorted. Group-level data effects predict and influence the behaviour of group members through algorithmic decision-making, and data contamination, data deviation or algorithmic impropriety may each make the conclusions of a group user profile diverge substantially from, or be wrong about, the users' real situation. Lacking any consideration of group-level data effects, the law cannot represent the interests of the members of that group. Suppose a group is defined as married women, and the data are set automatically to push lower-paid work to them. At the same time the "informed consent" mechanism of data collection fails, and the women in that group do not genuinely enjoy the right to "refuse the collection of their data"; the outcome of compulsory collection is ordinarily an unequal relationship between the data subject and the data collector and processor, and pressure is therefore exerted on different groups from various directions.

2. The absence of group-level data effects leads to the failure of the data relief procedure. Data governance emphasises individualism: "rights are inherently imbued with a strong individualist colour"[12]. The traditional view holds that modern society no longer permits single actions that damage the interests of the many to occur frequently, so that the framework which placed litigation between a plurality of parties has gradually fallen into disuse[13]. The absence of group-level data effects makes it difficult for an individual relief procedure to protect the group interest, and impossible to realise relief for the social harm data cause. First, the traditional relief procedure respects the autonomy of will of the data subject, but the infringement of data rights typically presents, so far as the data subject is concerned, a scattered character. The effect of a data infringement on a single data subject is slight, and on that premise the initiation of accountability proceedings is unlikely to be supported. Second, the externality of data is evident. Group-level data effects show that the social cost of data is not reflected in the cost of the individual transaction[14]; individual relief cannot complete the relief of the social harm caused by data infringement, and the complex relations of interest and composition of subjects radiate the effects of legal acts onto the group[15].

3 The Practical Predicament of Data Governance: The Individual Empowerment Model

3.1 The Individualism of the Model of Data Governance

Whether in China or abroad, theoretical discussion of data governance and institutional responses alike promise to return control of data to the data subject himself; choice, data freedom and self-control of data are to become the expected outcomes, data transparency is continuously strengthened, and rights continuously devolve so as to be transferred into the hands of network users. Data governance as a whole presents a strongly individualist character.

1. Conferring individual rights on the data subject. At present every model of data governance confers on the data subject the right to control data autonomously, and achieves this by imposing on service providers the obligations to notify,

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.

to permit inspection, and to collect, use and disclose personal data only after obtaining consent. Through this pairing of right and obligation the data subject may himself decide how to weigh the costs and benefits of collecting, using or disclosing information. The relevant normative documents—including the *Personal Information Protection Law*, the *Cybersecurity Law*, the *Data Security Law* and the "Data Twenty Articles"—regulate the collection and processing of data and all follow the governance model of "user empowerment"[16]; that is, the principal path chosen for data governance is to confer additional rights on the data subject (user empowerment) while fixing corresponding responsibilities on the data processor or collector. Article 41 of the *Cybersecurity Law*, for example, provides that without the consent of the person from whom they are collected, network operators may not collect or use personal information, and must otherwise bear the corresponding responsibility; the *Personal Information Protection Law* likewise emphasises that the consent of the individual must be obtained before personal information is collected; and the "Data Twenty Articles" stress, in respect of personal data, that "only under the authorisation of the data subject may a third-party subject collect and process" it—which in fact also follows the path of strengthening the individual rights of the data subject.

The "user empowerment" model means internalising data as the individual rights of the user and strengthening the autonomous rights the data subject enjoys over his data—that is, the right of data self-determination. The right of data self-determination strengthens the transparency of such actions as the collection and processing of personal data and makes clear the data subject's rights of information and choice, its purpose being to safeguard the autonomy of personal data processing.

2. Strengthening the premise of "informed consent" on the part of the subject. In order to strengthen the data subject's right of data self-determination, data governance throughout the world has followed a basic rule of personal information protection similar to "consent–informed". The European Union's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (95/46/EC)* (hereinafter the Free Movement Directive) emphasises the principle of autonomous decision by the information subject, providing that personal data may be processed only with the consent of the data subject[17]; the *General Data Protection Regulation*, as the most basic legal norm of personal data protection in the European Union, is a comprehensive expression of the purport of that protection and includes the right to be informed, the right of access, the right to object, the right of access to one's personal data and the right to be forgotten. Similar provisions include Germany's *Federal Data Protection Act*—"the collection, processing and use of data are lawful only with the consent of the data subject"; France's *Data Processing, Data Files and Individual Liberties Act (2004)*—"the processing of personal data must have the consent of the data subject…"; and the United Kingdom's *Data Protection Act*—"personal data may not be processed without consent or the satisfaction of other statutory conditions". Differing from the European Union and the European states, the United States grounds the protection of data in the protection of personal information and advocates preventing infringement through personal information self-determination, holding that "in view of the rapid development of internet and computer technology, self-regulation is the least intrusive and most effective means of ensuring fair information practices".

The European Union's model of data legislation revolves around power over personal data, while the data protection of the United States centres on the right of personal information self-determination. Although these two models of data protection are entirely distinct, both confer on the individual user control over data or information in order to realise data governance.

3.2 The Failure of the "User Empowerment" Model

Although the "user empowerment" model of data governance is applied by a number of countries, the governance path of "empowerment" essentially attenuates the legal interest in data into an individual rights claim of the data subject, and is in reality difficult to implement and to bring genuinely to the purpose of data governance; at the same time, an individual rights claim seeks individual relief when infringement occurs, and individual relief cannot protect the interest and effect of data at the group level. These points are elaborated below.

1. The empowerment path is difficult to delimit. The first paradox of "user empowerment" is that the empowerment path is difficult to clarify and the nature of the right difficult to define. When the empowerment of data was much debated, some scholars already observed that the cause of disputes over data lies in the unclear ownership of data rights; "without a clear definition of property rights there is no effective market", and confusion and contention arise accordingly[18]. But just what right should be conferred on data is a matter of wide disagreement. Some scholars propose treating data as a distinctive "thing", holding that the data holder enjoys ownership of the data it obtains through processing—that is, conferring a real right over data and placing data under the *Civil Code*. Yet data plainly do not satisfy the definition of a "thing", and the use of data is moreover incompatible with such characteristics of real rights as "one thing, one right" and "the right of the owner prevailing over the right of another", so that no civil right can be created[19]. When none of the other rights can achieve the protection of data interests, the empowerment path of personality rights must also be considered. "Informed consent" is the typical concretisation of the data personality right, but a data personality right would place the use

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.

and circulation of data entirely in the hands of the user; once the user refuses to disclose data, the circulation and exploitation of data will be obstructed by the predicament of information asymmetry that confronts the data user[20].

Although the model of data governance at the present stage still tends to proceed within the traditional legal framework, neither a property right nor a personality right (the mainstream modes of empowerment at present) is an ideal empowerment path. Conferring data rights will, because it "runs counter to the logical characteristics of the operation of the digital economy", "obstruct the free circulation of data, bring highly uncertain legal risk, and obstruct the development of the digital economy"[21]; at the same time the establishment of data rights readily produces "market barriers and restricts the free circulation of data"[22]. The establishment of data rights therefore "does not genuinely solve the problem of the circulation of data, but instead further strengthens the rights of the data controller, producing a de facto data monopoly"[23].

2. User rights are difficult to realise. The second paradox of "user empowerment" is that even if empowerment is possible, whether user rights can in fact be realised is highly uncertain.

First, users lack the capacity freely to decide upon and control data. Control measures centred on the right of data self-determination routinely fail: the processing of data is non-transparent, and the means of processing are secret and unknowable, so that information asymmetry exists between the user and the data collector and processor, breaking the user's right to decide upon his data[24]. Information asymmetry in the data market may perhaps be resolved by the rule of "informed consent", but a lack of control over personal data will in the end turn back upon "informed consent". When network users accept network services, the delivery of data is the consideration for obtaining services and products, so that there is almost no room for users to "not consent", and the realisation of personal data rights naturally becomes "empty talk". The prior duty to inform is also a means of alleviating the problem of information asymmetry, but the informing is usually effected by way of terms or contract: its content is not only extremely long and tedious but also full of vague wording, and such matters as the manner of data collection, the scope of application and the manner of processing are not clearly provided for, so that informing in such a case amounts to a dead letter.

Second, relief for data infringement is difficult. After conferring a certain data right on the user, how the fact of data infringement is to be relieved also presents practical problems. To begin with, differences in technical thresholds and in material resources exist between users and network service providers, and when the fact of infringement occurs, a relief method that relies on litigation cannot achieve the maintenance of rights. Some scholars have surveyed cases between 2017 and 2019 in which data subjects sought to vindicate their rights after a data breach, and found that in fewer than one quarter was the vindication successful, the principal reason being that users could not discharge the burden of proof[25]. The limited cognitive capacity of users makes the fact of data infringement difficult to prove, and the "black box" character of algorithms aggravates this predicament further. Next, the value of data is difficult to estimate: even if litigation succeeds, a court cannot accurately measure the value of data and so make a corresponding material compensation[26]. The value of data is difficult to determine because of the "scale" of data transactions and the difficulty of pricing data.

4 A Transformative Scheme for Data Governance: Group Data Governance

Group-level data effects supply the theoretical justification for group data governance, and experience from outside China may offer lessons for establishing a scheme of group data governance. On this basis a scheme of group data governance is established, proceeding from the preliminary stage of data governance, data collection, and the core mechanism and management mechanism of data governance.

4.1 Delimiting the Boundary of the Mechanism of Group Data Collection

The group interest in data presupposes a large aggregation of data, which necessarily involves the question of the lawful boundary of data collection. The group harmfulness that data production brings is bound up with its benefit: how to maximise the benefit of data production while averting the harm it brings is a question that must be answered. First, data governance should strengthen the reflection in personal data of effects on other data subjects: when an individual shares data, he must consider the effects on other data subjects and indeed on the whole group. Second, when internet platform enterprises evaluate and differentiate an aggregation of data, they should consider whether social discrimination and oppression will thereby arise. Third, the lawful boundary of compulsory data collection should be extended outwards to a certain degree. If the collection and processing of data, or the algorithm, may cause social harm and erode the data subject's self-expression and autonomous standing, then the collection and processing of data are unlawful. As for the compulsory collection of data, so long as it satisfies the group interest and does not produce an adverse effect on the data subject, it does not constitute unlawful collection even without the consent of the data subject. Corresponding normative rules therefore need to be formulated to represent the group interest, transforming data governance from the traditional right of the data subject to be forgotten, to obtain interests and to self-determine, into a recognised qualification to determine the purposes and conditions of data production, thereby establishing lawful mutual obligations[27].

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.

4.2 Establishing the Mechanism of Group Data Management

Some researchers hold that the European Union's proposed *Data Governance Act* permits data subjects to deliver their data rights to other data institutions, and therefore supplies a legal foundation for collective models of data governance. Such schemes include establishing compulsory public access to data or placing data in the public domain; other schemes advocate establishing unofficial public data-management bodies and managing data as a public rather than a private interest, which has produced the data trust. The world's first "data labour union" advocates collective data ownership, holding that only collective ownership can counter the many large data enterprises. Germany has also proposed the idea of establishing a national data trust, in the hope of countering the various technology enterprises that hold monopolies over personal data. The United Kingdom, Canada and other countries have all studied public data trusts, advocating the unified management of data as a collective resource[28]. Other research advocates data governance for the public interest, holding that after a certain number of years personal data should flow into the public domain to serve the public interest[29]. The advantage of the data trust scheme is that it can protect the private data rights of the data subject while also achieving data sharing, safeguarding the group interest in data, and establishing a complete and workable governance framework for the exchange and circulation of data.

1. The mechanism of data management: establishing a non-governmental Chinese data trust mechanism. The subject matter of the trust in a data trust should be data rights—that is, the trust institution should enjoy control over data rights (including the exchange and processing of data). This provision excludes data themselves from the scope of the trust, both because their own attributes remain disputed and because the value of data derives mainly from the processing of data, so that the protection of data themselves may rest on other norms[25]. Establishing a data trust mechanism can suspend the academic debate over whether data are a thing or property, and separate the dispute over the legal attributes of data from the tradability of data themselves[25]. In fact, the practice of taking a right as a form of intangible property within the scope of the subject matter of a trust has long had precedents, the most typical being equity trusts and the like.

The theoretical obstacle to a data trust is whether the transfer of the personality right within data rights is reasonable, which requires further thought. Article 1037 of the *Civil Code* provides for the information subject's right of erasure, and the *Shenzhen Special Economic Zone Data Regulations (Draft for Comment)* sets out in detail the right to inspect personal information, the right to erase personal information and the right to correct personal information; these rights belong to the part of personality rights, and it is generally held that personality rights are not alienable. In fact, however, in the internet era the transfer of part of one's data rights has long been the norm, and overemphasising the personality interest in data will obstruct the sharing and circulation of data and the optimisation of the allocation of data resources.

2. The mechanism of data use: using data around the "collective interest in data". Under group data governance the group interest that data safeguard stands above the individual interest of the data subject. First, the purposes of data use should be made clear. The purposes of data use should be differentiated by priority at the source: a purpose of use with a high priority may enjoy a higher authority to use data, and the scope within which compulsory collection may be carried out expands accordingly. Second, the conditions of data use should be made clear in order to delimit the subjects of data use. Large-scale data-processing activities require a certain resource background, so that enterprises of different scale may be granted different authorities to use data. Beyond enterprises, access to private data should be opened periodically to the national statistical department, in order to strengthen the contribution of data to the realisation of the public interest. Finally, clear standards of data confidentiality should be formulated, so as to safeguard in real terms the individual interest of the data subject.

3. The mechanism of public accountability: establishing a new mode of data supervision. Data governance needs to weigh better the relationship of interests between the freedom of data exploitation and the protection of data privacy, and establishing a mechanism for assessing group-level data effects has become one solution. A mechanism for assessing group-level data effects sets data exploitation between the two principal bodies of group-interest assessment and legal intervention, and conducts open and active monitoring and assessment of data identifiability, network intrusion and the degree of data disclosure. In conducting data supervision, the complexity of the interviewees, the visitors and other group members who may be affected should be taken into account, together with the nature and scope of the access activity, and supervisory measures appropriate to the sensitivity of the data covered should be adopted[50]. Google agreed to obtain project assessments "from qualified, objective and independent third-party professionals, using procedures and standards generally accepted within the industry", and Facebook agreed to a similar data protection plan. This can strengthen public awareness of the group, so that people have a clearer understanding of how their own data and interests will be affected by the group interest.

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.

5 Conclusion

Existing norms of data governance adjust the relationship between the data subject and the data collector and processor; they rely on user empowerment and safeguard the data interest through relief of the rights of the data individual. Yet the trend of the digital economy shows that the value of data derives more from the group characteristics of data obtained after collection and processing, which involve the interrelations among several data subjects, and that the individual empowerment model cannot achieve relief for data harm. Group-level data effects therefore need to be incorporated among the factors considered in data governance. This article places the centre of gravity of data governance on group-level data effects. First, it draws on the feasible experience of the data trust and, proceeding from the preliminary procedure and the core mechanism of data governance, makes clear the lawful boundary of data collection and establishes a non-governmental data trust. Second, it places the group interest of the data subject above the individual interest and enlarges the lawful scope of compulsory use of data. Third, it opens access to data periodically to designated institutions. Finally, it takes the mechanism for assessing group-level data effects as a fallback mechanism of accountability and supervision, and sets the criteria for assessing data within the group interest in data.

References

[1] Cohen J E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*[M]. New York: Oxford University Press, 2019.
[2] Ferreira A. The age of surveillance capitalism: the fight for a human future at the new frontier of power, by Shoshana Zuboff[J]. *Journal of Urban Affairs*, 2022, 44: 274-276.
[3] 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]
[4] Furlani A. The smart enough city: putting technology in its place to reclaim our urban future[J]. *The European Legacy*, 2022, 27(6): 1-2.
[5] Kitchin R. Big data, new epistemologies and paradigm shifts[J]. *Big Data & Society*, 2014, 1(1): 1-12.
[6] Boyd D, Crawford K. Critical questions for big data[J]. *Information, Communication & Society*, 2012, 15(5): 662-679.
[7] Viljoen S, Goldenfein J, McGuigan L. Design choices: mechanism design and platform capitalism[J]. *Big Data & Society*, 2021, 8(2): 27-34.
[8] Pasquale F. The black box society: the secret algorithms that control money and information[J]. *European Journal of Risk Regulation*, 2016, 7(2): 460-462.
[9] Paka P. Data management law for the 2020s: the lost origins and the new needs[J]. *Buffalo Law Review*, 2020, 68: 559-640.
[10] Harding S G. *Is Science Multicultural? Postcolonialisms, Feminisms and Epistemologies*[M]. Bloomington: Indiana University Press, 1998.
[11] Haraway D J. Situated knowledges: the science question in feminism and the privilege of partial perspective[J]. *Feminist Studies*, 1988, 14: 575-599.
[12] Zhou Y L. On the history of the concept of rights[J]. *Journal of the Graduate School of the Chinese Academy of Social Sciences*, 1985(4): 18-26. [in Chinese]
[13] Cappelletti M. Vindicating the public interest through the courts: a comparativist's contribution[J]. *Buffalo Law Review*, 1975(25): 519.
[14] Solove D J. Privacy self-management and the consent dilemma[J]. *Harvard Law Review*, 2013, 126(7): 1880-1903.
[15] Zhang Q Y. A review of new rights and the rise of obligations: the perspective of group rights[J]. *Frontiers*, 2021, 47(1): 144-151. [in Chinese]
[16] Xu K. A retrospective and reflection on the anniversary of the European Union's General Data Protection Regulation[J]. *Electronic Intellectual Property*, 2019(6): 4-15. [in Chinese]
[17] Chen F. *Personal Data Protection: The EU Directive and Member State Law, and the OECD Guidelines*[M]. Beijing: Law Press, 2006. [in Chinese]
[18] Xu K. Three approaches to data protection: a comment on the unfair competition case of Sina Weibo v. Maimai[J]. *Journal of Shanghai University (Social Sciences Edition)*, 2017, 34(6): 15-27. [in Chinese]
[19] Mei X Y. The legal attributes of data and their civil-law positioning[J]. *Social Sciences in China*, 2016(9): 164-183. [in Chinese]
[20] Posner R A. The economics of privacy[J]. *American Economic Review*, 1981, 71(2): 405-409.
[21] Fu X H. A critique of the theory of protecting enterprise data property rights: from data property rights to data use rights[J]. *Oriental Law*, 2022(2): 1674-4039. [in Chinese]
[22] Mei X Y. An original theory of enterprise data interests: from property to control[J]. *Peking University Law Journal*, 2021, 33(5): 1188-1207. [in Chinese]
[23] Jin Y. Reflection on and advance of the legal path of data governance[J]. *Law Science*, 2020, 38(2): 79-89. [in Chinese]
[24] Ren L L. On consent not being the legitimate basis for the processing of personal information[J]. *Politics and Law*, 2016(1): 126-134. [in Chinese]
[25] Feng G, Xue Y S. The data trust from the "rights-norm model" to the "conduct-control model": another approach to constructing a mechanism for protecting the rights of the data subject[J]. *Law Review*, 2020, 38(3): 70-82. [in Chinese]
[26] Delacroix S, Lawrence N D. Bottom-up data trusts: disturbing the "one size fits all" approach to data governance[J]. *International Data Privacy Law*, 2019, 9(4): 236-252.
[27] Hardimon M O. The struggle for recognition: the moral grammar of social conflicts, by Honneth[J]. *Journal of Philosophy*, 1997, 94(1): 46-54.
[28] Sadowski J, Viljoen S, Whittaker M. Everyone should decide how their digital data are used—not just tech companies[J]. *Nature*, 2021, 595(7866): 169-171.
[29] Shah H. Use our personal data for the common good[J]. *Nature*, 2018, 556(7699): 7.
[30] Keller P. The reconstruction of privacy through law: a strategy of diminishing expectations[J]. *International Data Privacy Law*, 2019, 9(3): 132-152.

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.