A STUDY ON THE REGULATORY PATHWAY FOR THE CIRCULATION OF ELDERLY-RELATED DATA UNDER THE EMERGING INTEGRATED MEDICAL AND ELDERLY CARE MODEL

Tan Ji

TABLE OF CONTENTS

I. INTRODUCTION ····· 58
II. STRUCTURAL CLARIFICATION:
RECONFIGURING LEGAL RELATIONS IN THE NEW INTEGRATED
MEDICAL AND ELDERLY CARE SERVICE MODEL ····· 61
III. PRACTICAL DIFFICULTY:
PROBLEMS IN THE FLOW OF ELDERLY-RELATED DATA WITHIN
INTEGRATED MEDICAL AND ELDERLY CARE SERVICES ····· 63
A. Data Service Authorisation:
Fragmentation in Legislative Regulation ····· 63
B. Data Transmission and Operation:
The Weakening of the Subject Status of Data Right-Holders ····· 65
C. Data Supervision and Safeguard:
Regulatory Inadequacy of Related Departments ····· 68
IV. REGULATORY PATHWAY:
CONSTRUCTING A DUAL-TRACK AND MULTI-STAKEHOLDER
GOVERNANCE FRAMEWORK FOR ELDERLY-RELATED DATA ····· 70
A. Top-Down Legal Reform ····· 72
B. Bottom-Up Institutional Innovation ····· 73
C. Multi-Stakeholder Governance and Full-Chain Protection ····· 78
V. CONCLUSION ····· 82

A STUDY ON THE REGULATORY PATHWAY FOR THE CIRCULATION OF ELDERLY-RELATED DATA UNDER THE EMERGING INTEGRATED MEDICAL AND ELDERLY CARE MODEL

Tan Ji[*]

Within the new model of integrated medical and elderly care services, elderly-related data manifest a composite rights structure that integrates both public and private law dimensions. The granular and multi-dimensional nature and heightened sensitivity of such data, combined with the inherent vulnerability and dependency of elderly-related data subjects, render the regulatory landscape particularly complex. Existing mechanisms for data circulation reveal deficiencies, including fragmented legal norms, indeterminate allocation of data ownership, and supervisory inadequacy. This paper conducts a doctrinal inquiry into the legal relationships among multiple stakeholders across three principal dimensions: data service authorisation, data transmission and operation, and data supervision and safeguard. It proposes a regulatory framework based on a dual-track mechanism—combining top-down harmonisation of existing legal provisions with bottom-up implementation of data trusts—supported by a comprehensive oversight architecture involving government agencies, public interest organisations, and industry associations. This framework is intended to ensure the effective protection of the rights and interests of digitally vulnerable elderly individuals.

I. INTRODUCTION

Amid the rapid transformation of Chinese society into a super-aged demographic structure, elderly-related data have emerged as a key productive element in addressing the structural imbalance between the supply of and demand for eldercare resources, while also enabling the precision-based implementation of intelligent medical and nursing services. According to the *Fifth Sample Survey on the Living Conditions of the Elderly in Urban and Rural China*, approximately thirty-five million elderly persons, representing

* Associate Professor at School of Artificial Intelligence and Law of Southwest University of Political Science and Law.

11.6 percent of the total elderly population, are classified as the disabled.[1] A significant proportion of this population relies on intelligent monitoring devices for real-time health management and emergency response. This demographic and technological reality compels the adoption of integrated service models based on technologies such as the Internet of Things and artificial intelligence, thereby establishing a closed-loop data system in which elderly-related data form the central component across the entire cycle of 'collection, analysis, and application'.

Elderly-related data encompass multiple domains. First, health-related data refer to physiological indicators and medication records. Second, lifestyle-related data include behavioural trajectories and social interaction patterns. Third, rights-related data concern the individual's caregiving context, economic capacity, and family support structure. These data categories are intimately tied to the fundamental rights of elderly individuals, including the right to life and health, the right to privacy, and property rights. Accordingly, elderly-related data exhibit a dual legal character, simultaneously bearing the attributes of personality rights and proprietary interests. The lawful and ethical governance of such data thus implicates a broader normative balance between the personal information protection framework articulated in article 1034 of the *Civil Code of the People's Republic of China* (hereinafter referred to as the Civil Code) and the policy objective of effective assistance to the elderly as set forth in the *Law on the Protection of the Rights and Interests of the Elderly*.

Despite their growing significance, elderly-related data governance faces three systemic regulatory dilemmas. The first concerns a deficit in norm supply. The *Personal Information Protection Law* and the *Data Security Law* lack differentiated provisions tailored to the specific vulnerabilities of elderly-related data subjects. They do not provide special safeguards for biometric or sensitive health information, nor do they offer interpretive guidance concerning the capacity for consent in complex scenarios involving digital agents or implied consent mechanisms.

The second dilemma pertains to the challenge of balancing competing interests. The boundary between the public interest served by data utilisation and the private interests of elderly individuals remains ill-defined. In practice, this ambiguity has led to the formalisation of consent procedures and the widespread use of static, one-time risk assessments. It is not uncommon for

1 Zhao Zhenqi, *Let the Elderly Can Enjoy a Happy Old Age: The State Council's Report on Promoting the Construction of the Elderly Service System and Strengthening and Improving the Care for the Disabled*, 19 The People's Congress of China 35, 35-37 (2024).

eldercare institutions to condition the provision of services on compulsory data authorisations, and for technology firms to engage in profiling that exceeds the scope of consent originally granted.

The third dilemma concerns the inadequacy in regulatory oversight. Existing supervisory mechanisms need to provide comprehensive regulation across the full data lifecycle. The oversight inadequacy heightens the dual risks of 'data silos' and 'algorithmic opacity', undermining both institutional accountability and individual protection.

In response to these challenges, legal scholars have advanced differing doctrinal approaches. From a civil law perspective, some scholars advocate for the categorisation of personal information and the adoption of a reversed burden of proof, drawing on the principles of informed consent, public interest, and party autonomy.[2] Others argue for participatory governance mechanisms that incorporate public interest organisations and industry associations, supported by frameworks grounded in the *Government Procurement Law* and formalised through internal charters. From an administrative law perspective, commentators have called for the development of a people-centred, law-based government capable of coordinating regulatory functions across various administrative levels and integrating grassroots communities into the data governance process.[3]

While these efforts have enriched the debate, existing scholarship remains largely confined to one-dimensional models, focusing either on civil law remedies or administrative regulation. Two major limitations are particularly evident. First, the overemphasis on procedural compliance with informed consent requirements neglects the substantive inability of cognitively impaired elderly individuals to make autonomous data decisions. Second, the mechanical transplantation of generic personal data governance paradigms fails to respond to the unique ethical, familial, and intergenerational dimensions embedded in elderly-related data. This institutional misalignment—where regulatory frameworks lag behind technological development—demands a more adaptive and multidimensional governance architecture.

Against this backdrop, the present study examines the collection, management, and utilisation of elderly-related data within integrated medical and eldercare services. It aims to clarify the legal relationships among the

2 Si Dan, *Civil Law Protection of the Elderly in the 'Internet + Pension' Model*, 2 Business & Economy 140, 139-140 (2021).

3 Xu Ke, *Ternary Governance of Data Transaction Circulation: Technology, Standard and Law*, 43(1) Journal of Jishou University (Social Sciences) 96, 97-104 (2022).

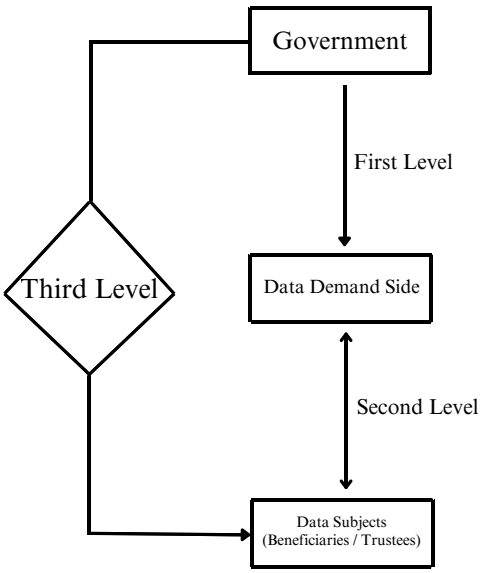
multiple actors involved, assess the regulatory deficits present in current practices, and explore the feasible pathway for safeguarding the personal data of digitally disadvantaged elderly groups. Framed within a model that promotes the integration of medicine, nursing, and education, this inquiry seeks to bridge the normative gap between rapid technological advancement and relatively static architecture of existing legal institutions.

II. STRUCTURAL CLARIFICATION: RECONFIGURING LEGAL RELATIONS IN THE NEW INTEGRATED MEDICAL AND ELDERLY CARE SERVICE MODEL

As a socially oriented public service model, the new type of integrated medical and elderly care service (hereinafter referred to as the IMECS) demonstrates a clear evolution toward the diversification of actors and the hybridisation of service content. In terms of actors, the traditional model primarily involves a binary legal relationship between eldercare institutions and elderly individuals, while medical institutions remain external collaborators without being incorporated into the core framework of contractual rights and obligations. In the IMECS framework, however, service delivery depends on the coordinated participation of medical institutions, eldercare institutions, elderly individuals, family members and insurance providers, forming a multi-actor collaborative network. Regarding service content, conventional arrangements focused mainly on daily living assistance, with medical services limited to emergency intervention. This division reflected a functional and contractual separation between ‘medical’ and ‘care’. In contrast, the IMECS model provides a full-cycle, integrated service package encompassing prevention, treatment, rehabilitation and hospice care.

From the perspective of legal relationships, the circulation and governance of elderly-related data within the IMECS generate multiple intersecting legal relations among three primary actors: the government, data demanders (namely IMECS-related institutions), and data subjects (elderly service recipients or their authorised representatives). Given the heterogeneity of these relationships, the data governance structure within the IMECS may be analytically divided into three interrelated levels: data service authorisation, data transmission and operation, and data supervision and safeguard (see Figure 1).

Figure 1: Three-Tier Legal Relationships Governing Elderly-Related Data Flow in Integrated Medical and Elderly Care Services



At the authorisation level, the legal relationship exhibits a distinct public law nature. Medical and eldercare institutions, as data demanders, generally obtain their rights to process elderly-related data through administrative concessions granted by the state. This process forms an administrative franchising relationship between the government and the institutions.[4] The government plays a central role in policy formulation, resource allocation, and safeguarding institutional stability and goal attainment. Despite the government's dominant position in this relationship, elderly individuals occupy a position of indispensable significance. As both the providers of data and the ultimate beneficiaries of services, their interests must be safeguarded during the exercise of public authority. In particular, the government must ensure that data collection is lawful, necessary and proportionate, and that the elderly's right to informed consent is respected in both procedural and substantive terms.

The second level, namely data transmission and operation, reflects a mixed legal structure combining both public and private law attributes. On the private law side, data subjects and data demanders may enter into licensing agreements or authorisation arrangements for the transfer and use of

4 Cao Huimin & Deng Tingting, *Research on Government Data Governance Risk and Its Resolution Mechanism*, 217(1) E-Government 86, 86-90 (2021).

elderly-related data.[5] Although elderly individuals often possess relatively weak bargaining power, no hierarchical subordination exists between the parties. The conclusion of such agreements is based on the voluntary and autonomous will of the data subjects, which affirms the private law character of these relationships. From the public law perspective, the IMECS is fundamentally a public interest-oriented system. Therefore, the role of government remains essential not only in authorisation but also throughout the data transmission process. Administrative oversight is required to ensure service quality, protect personal data rights and maximise social benefit. This hybrid nature demands a regulatory framework that simultaneously preserves the individual rights of elderly persons and guarantees the operational integrity of the public service.

The third level, data supervision and safeguard, is characterised by a predominantly public law regulatory relationship. In the traditional model, the state acted as the main provider and financier of public services. With the rise of the service-oriented government model, the state has progressively adopted socialised supply mechanisms. Nonetheless, the fundamental objective of protecting the rights and interests of elderly individuals has remained unchanged. In this context, the state establishes dedicated administrative review and supervisory mechanisms to convert the abstract goal of elderly protection into concrete administrative obligations. This regulatory model, backed by state coercive authority, reshapes the power dynamics within the IMECS data governance ecosystem. Public law norms become the primary source of legitimacy for regulatory action. As regulatory enforcement strengthens, the nature of the legal relationships within this dimension increasingly returns to its foundational public law character.

III. PRACTICAL DIFFICULTY: PROBLEMS IN THE FLOW OF ELDERLY-RELATED DATA WITHIN INTEGRATED MEDICAL AND ELDERLY CARE SERVICES

A. Data Service Authorisation: Fragmentation in Legislative Regulation

The current legal framework remains insufficient to meet the evolving informational demands of intelligent eldercare services. On January 11, 2024, the General Office of the State Council issued the *Opinions on Developing the Silver Economy and Enhancing the Well-Being of the Elderly*, explicitly

5 Yao Leye, *Smart Pension Data Resource Element Identification, System Architecture and Scenario-Based Application*, 46(1) Information and Documentation Services 21 (2025).

advocating the creation of new formats for smart health and eldercare and encouraging the application of next-generation information technologies and intelligent devices in such settings.[6] Realising these objectives inevitably involves the extensive collection and analysis of physiological indicators, behavioural records, and mental state data through interconnected systems based on the Internet of Things and related digital infrastructures. However, the statutory regime governing these processes exhibits structural gaps.

At present, the *Law on the Protection of the Rights and Interests of the Elderly*—the central legal instrument for safeguarding elderly rights—does not contain a general clause addressing the protection of elderly personal information. Its provisions are limited to broadly framed goals, such as ensuring the lawful rights and interests of older persons and promoting contributions from all sectors of society. It does not provide a targeted legal framework specifically designed to address personal data rights. Other legislative instruments similarly lack provisions dedicated to the unique data protection needs of elderly persons. Although the *Personal Information Protection Law* establishes a general framework based on the principle of informed consent, the specific legal bases for data processing enumerated in article 13 are difficult to operationalise in the context of intelligent eldercare.

China's existing regulations concerning personal information protection are primarily formulated for conventional Internet enterprises. For example, the *Provisions on the Protection of Personal Information of Telecommunications and Internet Users* establish baseline protection from the perspective of telecommunications services but are limited in scope to traditional data use in the provision of Internet-related services. These rules do not extend to data collected through intelligent devices in Internet of Things environments. Similarly, the *Assessment Standard for Personal Information Protection by Internet Enterprises*, which was developed to implement the *Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Online Information*, applies exclusively to traditional Internet firms and does not adequately address the novel data governance challenges presented by intelligent eldercare technologies.

Beyond these situations, the procedural safeguards for personal data collection remain underdeveloped. In practice, *ex ante* legal requirements often diverge from technological realities. Article 17 of the *Personal Information Protection Law* imposes comprehensive disclosure obligations

6 General Office of the State Council of the People's Republic of China, *Opinions of the General Office of the State Council on Developing the Silver Economy and Improving the Well-Being of the Elderly*, No. 1 [2024] of the General Office of the State Council.

on telecommunications operators and Internet service providers, yet these obligations are difficult to realise in practice. As platforms increasingly standardise lengthy privacy notices, elderly users—due to cognitive decline or limited digital literacy—often lack the capacity to fully understand or even review such disclosures. According to one empirical study, an average user would require more than two hundred hours per year to read all privacy policies encountered online.[7] This burden is clearly incompatible with the expectations and capacities of elderly users.

The data collection environment in intelligent eldercare services further complicates the matter. Internet of Things devices routinely capture highly sensitive categories of information, including biometric, health, and behavioural data, often under broad and vaguely defined user agreements. These agreements frequently fail to specify the purpose, scope, and duration of data processing activities, thereby depriving elderly individuals of meaningful control over their personal information. For example, many smart health monitoring devices automatically transmit user data to external servers without transparent explanation or specific consent procedures. In such cases, elderly persons may unintentionally lose control over their most sensitive data. This is particularly concerning given their enhanced vulnerability, both physically and cognitively. In light of these conditions, the refinement of procedural safeguards for elderly-related data collection and authorisation has become a matter of both legal necessity and ethical urgency.

B. Data Transmission and Operation: The Weakening of the Subject Status of Data Right-Holders

Personal data contain not only the personality-related interests of data subjects but also increasingly significant proprietary value. However, the potential for value appreciation and the inherent alienability of data fundamentally challenge the legal logic underpinning both tangible property protection and traditional personality rights. Personality rights are typically understood to entail exclusive and indivisible control by the rights-holder, whereas data, by contrast, may be reproduced, transmitted, and utilised through a wide range of channels. This hybrid nature complicates the legal demarcation of ownership, control, and use rights over personal data, often rendering such boundaries vague and indeterminate.

In recent years, policy developments have begun to address this legal

7 Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 Journal on Telecommunications & High Technology Law 273, 274 (2012).

ambiguity. The *Opinions of the Central Committee of the Communist Party of China and the State Council on Building Basic Systems for Data and Giving Full Play to the Role of Data Resources* offer high-level strategic guidance. The document calls for the establishment of classified and hierarchical systems for confirming data rights, promoting authorised use, and enabling the market-oriented circulation and trading of data. While this signals an emerging framework for data governance, the actual legal pathways through which different actors can assert, transfer, or protect their interests in data remain largely undefined. In the absence of detailed rules and operative mechanisms, actors in the data transaction chain face uncertainty regarding their legal status and corresponding protection.

At the statutory level, current Chinese legislation—particularly the *Personal Information Protection Law* and the *Cybersecurity Law*—primarily adheres to a notice-and-consent model as the foundational basis for legitimising the collection, processing, and transfer of personal data. This model appears to affirm the exclusive control of individuals over their data by requiring that their informed consent be obtained prior to any processing activity. In substance, however, this structure sometimes fails to deliver effective autonomy or protection, especially for elderly individuals.

Due to cognitive decline, information asymmetries, and limited digital literacy, many elderly persons are unable to fully comprehend consent agreements or exercise meaningful agency in data-related transactions. This weakens their role as autonomous rights-holders and places them in a structurally disadvantaged position within the data ecosystem. Furthermore, because the consent model operates on a case-by-case basis and lacks a coherent framework for systemic coordination, it contributes to the fragmentation of data resources across institutional boundaries. As a result, the accumulation of data silos becomes a structural by-product of individualised consent, impeding the effective integration and ethical governance of elderly-related data in medical and care settings. In light of these challenges, there is a pressing need to rethink the current legal model governing data transmission and to explore mechanisms that can more robustly protect the status of data subjects—particularly vulnerable groups such as the elderly. This includes considering alternatives to consent-based paradigms, such as public trusteeship models, fiduciary duties for data controllers, or collective negotiation mechanisms, to ensure that the informational autonomy and legal subjectivity of elderly individuals are not merely formalistic, but substantively realised.

From a practical perspective, the existing legal framework—although

formally comprehensive—remains substantively abstract, resulting in a gap between legally enshrined rights and their effective enforcement in real-world settings. Ideally, elderly persons, as data subjects, should stand on equal legal and factual footing with data controllers, including smart eldercare service providers and device manufacturers. This parity would enable them to meaningfully negotiate the terms of data use and to share in the benefits of data-driven services. In reality, however, elderly individuals occupy a structurally inferior position within the digital contractual framework. This asymmetry arises from compounded psychological and physiological vulnerabilities, which significantly impair their ability to comprehend, assess, and contest contractual terms or data practices. The imbalance in bargaining power between elderly users and commercial entities has become both widespread and deeply embedded in current digital service ecosystems.[8]

At the statutory level, article 1038 of the Civil Code grants natural persons the right to prevent the unauthorised or arbitrary processing of their personal information. It further provides that data handlers are prohibited from disclosing, altering, or unlawfully transmitting personal data without the informed consent of the individual concerned. Exceptions are permitted only where the data have been anonymised to the extent that no specific individual can be identified and re-identification is no longer feasible. Despite these legal guarantees, elderly persons often face significant procedural and evidentiary burdens when attempting to assert their rights. In particular, establishing a viable information tort claim requires the claimant to demonstrate the occurrence of specific elements such as unlawful processing, actual harm, and causation. These requirements pose substantial challenges for elderly claimants, who typically lack both technical expertise and access to relevant evidence. In contrast, data controllers often enjoy a position of institutional advantage and face minimal legal consequences in the absence of formal litigation or regulatory intervention.[9]

This enforcement imbalance underscores a core weakness in the prevailing consent-based data governance paradigm. While the model purports to empower data subjects through the mechanism of informed consent, it does little to address the evidentiary difficulties involved in proving data misuse or to impose sufficient deterrent costs on data controllers who violate legal obligations. As a result, the consent model

8 Wang Ye, *Digital Divide and the State Protection of Digitally Disadvantaged Groups*, 5 Journal of Comparative Law 121, 121-137 (2023).

9 Liu Quan, *On the Principle of Legality, Legitimacy and Necessity of Personal Information Processing*, 5 The Jurist 10, 10-13 (2021).

often functions as a procedural formality rather than a substantive safeguard, failing to protect the most vulnerable groups in practice.[10] In this context, enhancing the legal status and practical capacity of elderly-related data subjects requires a shift beyond traditional paradigms toward more robust institutional protection, procedural presumptions in favour of data subjects, and affirmative duties of care on the part of data controllers.

From the perspective of social utilisation, personal information in the data era is not merely a private asset but also a vital component of shared societal resources. Individualised and fragmented data attain their greatest value only through continuous circulation, integration, and application across multiple functions.[11] If consent is treated as the sole legal basis for processing elderly-related data, the costs of obtaining that consent may become prohibitively high, thereby undermining the efficiency of digital eldercare services and hindering industrial development. An excessively high consent threshold impedes effective data use, diminishes service quality and innovation capacity, and imposes significant constraints on the sustainable growth of the digital eldercare economy.[12]

C. Data Supervision and Safeguard: Regulatory Inadequacy of Related Departments

As a national strategic response to the challenges of a super-aged society, the development of intelligent eldercare services significantly implicates the rights and interests of approximately 280 million elderly individuals in China. The efficacy of data supervision in this domain directly affects the realisation of those rights. However, regulatory inadequacy in the governance of smart eldercare data reveals issues such as administrative fragmented oversight. These problems are rooted in a structural mismatch between the traditional regulatory model and the operational logic of emerging data-based governance.[13]

First, institutional fragmentation within the regulatory architecture has constrained the overall effectiveness of data governance. Pursuant to the regulatory arrangement established by the *Opinions on Further Advancing the Development of Integrated Medical and Elderly Care*, a dual-track

10 Feng Guo & Xue Yisa, *Data Trust from 'Rights Regulation Mode' to 'Behavior Control Mode': Another Idea of Building Data Subject Rights Protection Mechanism*, 38(3) Law Review 72, 72-73 (2020).

11 Gao Fuping, *Data Circulation Theory: Foundation of Data Resource Right Allocation*, 31(6) Peking University Law Journal 1410, 1410-1411 (2019).

12 Ren Longlong, *On the Issue That Consent Is Not the Legitimate Basis of Personal Information Processing*, 1 Political Science and Law 130, 130-132 (2016).

13 Gao Xiaoping, *Big Data Induced Governance Reform and Innovation*, 10 Chinese Public Administration 10, 10-14 (2015).

system has been implemented. Under this model, the health departments primarily focus on the compliance of medical data, while the civil affairs departments are responsible for regulating the quality of eldercare service data. However, newly generated data elements—such as real-time health monitoring data and behavioural tracking data—possess both clinical diagnostic significance and eldercare service relevance. Because integrated medical and elderly care services inherently combine medical and caregiving functions, the data collected reflect hybrid character and entail complex and high-volume regulatory demands. Institutions must simultaneously undergo scrutiny by multiple agencies, including those responsible for medical insurance, emergency management, and market regulation. In practice, inter-agency regulatory cooperation is hindered by fragmented administrative functions, leading to overlapping responsibilities, operational redundancies, and jurisdictional conflicts. The cross-sectoral nature of data in this field further obscures lines of regulatory accountability. Different departments sometimes lack consensus on responsibility attribution, resulting in stagnation in enforcement decision-making. A more pressing concern is the lack of unified standards for data collection by different regulatory bodies. This inconsistency renders interdepartmental data integration difficult, leading to fragmented and incompatible data repositories. In turn, this limits the ability of authorities to process, analyse, and interpret data effectively, and thus weaken collaborative supervision mechanisms and impede the development of an integrated and responsive cross-departmental data governance model.

Second, existing regulatory tools have not kept pace with the speed and complexity of data flows. The prevailing supervisory approach continues to mainly rely on traditional means, including on-site inspections and the verification of paper-based records.[14] These methods are not suitable enough for the regulation of intelligent eldercare data, which are characterised by real-time generation, multisource heterogeneity, and high-frequency updating. In current practice, data collected by eldercare institutions must be synchronised with platforms operated by multiple regulatory bodies, including the civil affairs department's eldercare quality supervision system, the health department's chronic disease management system, and the cybersecurity administration's personal information protection platform. However, due to incompatible system interfaces and the absence of standardised integration protocols, data synchronisation is occasionally delayed. This results in the loss of real-time value for critical data, such as fall alerts or medical alarms,

14 Liu Jianyi, *Big Data-Driven Innovation of Government Supervision and Regulation*, 26(5) Administrative Tribune 102, 102-107 (2019).

thereby undermining the timely intervention capacity of regulators.

Third, the lack of a robust regulatory accountability framework may increase the risk of data misuse. Although the *Cybersecurity Management Measures for Medical and Health Institutions* stipulate the principle of primary responsibility—where regulatory authority and supervisory duty are aligned—the practical implementation of this principle is often obstructed by the complex and multilayered nature of data ecosystems in intelligent eldercare. Data chains typically involve device manufacturers, network operators, eldercare institutions, and medical service providers. In such a context, clearly delineating responsibility boundaries is difficult. Regulatory closure is also at risk of fragmentation, as different departments may handle the same incident through inconsistent procedures or assessment criteria. This segmented regulatory approach is fundamentally misaligned with the full-lifecycle governance requirements of intelligent eldercare data. As a consequence, violations involving data collection, use, or transmission are often difficult to trace to specific accountable parties.

IV. REGULATORY PATHWAY: CONSTRUCTING A DUAL-TRACK AND MULTI-STAKEHOLDER GOVERNANCE FRAMEWORK FOR ELDERLY-RELATED DATA

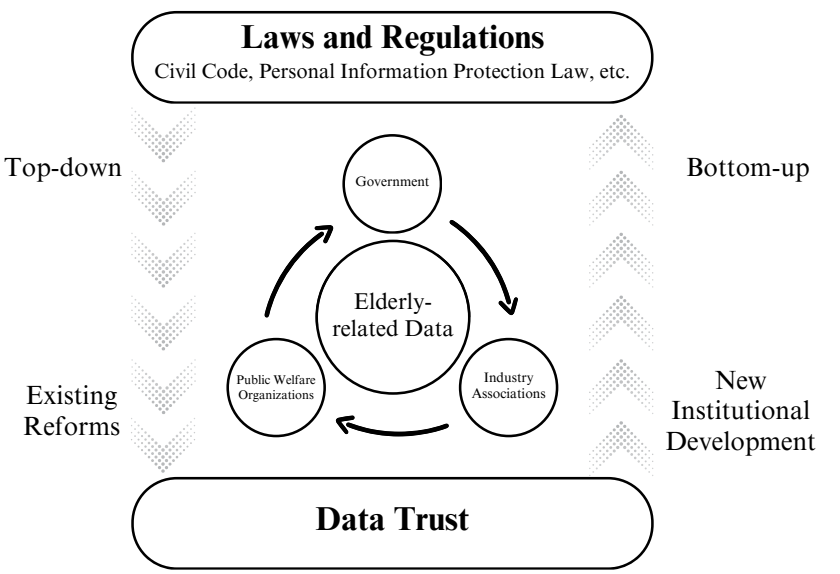
In order to address the diverse regulatory challenges present within the new integrated model of medical and elderly care services, this study proposes the establishment of a governance framework for elderly-related data that centres on a dual-track regulatory pathway and the involvement of pluralistic regulatory actors. This framework is grounded in the realities of current data circulation practices and aims to provide both institutional coherence and operational feasibility.[15] On the one hand, the collection, use, and management of elderly-related data require not only top-down reforms of existing legal and regulatory instruments but also bottom-up innovation in governance mechanisms. Specifically, while it is essential to revise and refine the statutory and regulatory frameworks that govern data processing activities, it is equally important to explore grassroots-oriented institutional innovations. One such approach involves the introduction of third-party trust institutions into the existing integrated care model and the establishment of a digital trust regime. By creating a system of data trusteeship, elderly-related

15 Hao Tao, Shang Qian & Li Jing, *A Study on the Effective Supply Path of Combining Medical Care with Elderly Care Services Under PPP Mode*, 11 Macroeconomics 44, 44-52 (2018).

data can be afforded more comprehensive legal and technical protection throughout their lifecycle, thereby enhancing the overall accountability and transparency of data use in eldercare services.

On the other hand, in addition to the traditional public service model dominated by governmental supervision, this study advocates for the active engagement of non-state actors, including public interest organisations and industry associations, in the multi-level protection of elderly-related data. These entities should assume a greater share of social responsibility by participating in oversight processes, standard-setting initiatives, and the formulation of internal compliance rules relevant to data ethics and security in eldercare contexts. Their involvement can serve as a necessary supplement to governmental supervision, contributing to the development of a more resilient and inclusive regulatory ecology. This multidimensional regulatory strategy is designed to ensure that elderly-related data are supported by legal norms and technical safeguards at every stage of processing. It also seeks to foster a collaborative environment in which diverse actors across the public and private sectors can contribute to the development of a secure, rights-respecting, and trustworthy data infrastructure for elderly populations. Ultimately, the objective is to construct a comprehensive regulatory ecosystem that both protects the digital rights of elderly individuals and promotes the sustainable growth of smart eldercare services (see Figure 2).

Figure 2: Dual-Track Governance Framework for Elderly-Related Data



A. Top-Down Legal Reform

To effectively regulate elderly-related data within intelligent eldercare services, the legal and regulatory framework must comprehensively respond to the sector's evolving informational demands and reflect the objectives set out in current policy directives concerning the well-being of older persons. The *Opinions on Developing the Silver Economy and Enhancing the Well-Being of the Elderly* highlight the essential role of the Internet of Things in building smart eldercare models. The realisation of this objective requires legislative initiatives that supplement and support technological development with institutional safeguards.

First, the existing framework for personal information protection in China is primarily oriented toward the telecommunications and Internet service sectors. The relevant provisions largely apply to telecommunications business operators and providers of Internet information services. However, they do not extend to other key actors within the smart eldercare ecosystem, such as public institutions, healthcare providers, and Internet of Things service platforms. This regulatory limitation may influence the formation of a comprehensive legal system capable of addressing the full data lifecycle within smart eldercare scenarios.[16] Accordingly, legislation should be promptly expanded to cover all stages of intelligent eldercare operations. The state should issue specific legal norms on data protection tailored to the smart eldercare context. On the basis of the existing *Government Procurement Law*, a dedicated legal framework should be developed to regulate the collection and use of elderly-related data in public service contracts. This framework should clearly define the preconditions for data collection, procurement procedures, and the structural configuration of data-related components in eldercare projects. By doing so, it would promote both the lawfulness and transparency of data usage practices.

Second, the issue of concealed data collection by Internet of Things service providers during the data acquisition phase warrants legislative attention. Current practice may not always fully inform elderly users about the nature and scope of data being collected. Given the limited cognitive and educational capacity of many older individuals, they may not be in a position to understand or assess the terms of complex authorisation agreements. To address this concern, legislation should specify the responsibilities and legal obligations of Internet of Things service providers and related platforms in

16 Zhang Jingtang & Rui Guoqiang, *Smart Health Care Driven by Big Data: Realistic Representation, Internal Elements and Optimization Path*, 5 Social Sciences in Hunan 136, 136-140 (2023).

the context of smart eldercare. A more rigorous procedural framework should be introduced, including the establishment of a data collection authorization list mechanism. Under this approach, all data collection activities would be subject to prior review and approval by designated government authorities. This system would function as a substitute for individual review by elderly users and thereby enhance the reliability and legality of the data collection process. In addition, it is necessary to improve the information disclosure regulations applicable to relevant government departments. These rules should guarantee that elderly individuals and their legal guardians may at any time monitor and inquire about ongoing data collection activities. Such measures would enhance transparency, foster public trust, and promote meaningful user participation.[17]

Third, the government should develop a specific legal framework governing both the collection of elderly-related data and the broader provision of intelligent eldercare services, using the existing *Government Procurement Law* as a foundation. This framework should stipulate the basic legal conditions for data collection, standardise the procurement process, and define the overarching legal structure of smart eldercare programmes. While the law should set the core parameters, it should also permit flexibility in contractual negotiation with respect to data-related matters, such as the scope of use, collection methods, and technical requirements. So long as these terms remain compliant with applicable laws and regulations, allowing such discretion can help balance legal legitimacy with market efficiency, thereby facilitating the lawful and effective circulation and use of elderly-related data.

B. Bottom-Up Institutional Innovation

1. Toward a Framework for Treating Elderly-Related Data as Public Data Trusts. — The data governance paradigm centred on data trusts offers a more comprehensive regulatory structure. At present, the principal governance models in the global discourse include data trusts, data cooperatives, and corporate or contractual mechanisms. Compared to data cooperatives built upon voluntary contracts or corporate entities, data trusts provide stronger legal safeguards. Likewise, in contrast to corporate or contractual models that promote data sharing to achieve specified objectives

17 Chen Yi, *Research on Healthcare Data Sharing and Personal Information Protection*, 42(5) Journal of Intelligence 192, 192-198 (2023).

or serve public interests,[18] data trusts are more precisely oriented toward the protection of the rights and interests of data principals.[19] This stronger form of protection, when deployed within existing legal frameworks, is particularly well-suited to the needs of elderly individuals. It reflects a normative vision of safeguarding vulnerable populations and strengthens the availability and enforceability of private rights-based remedies.

On the one hand, trust law jurisprudence provides a superior normative framework for overcoming the limitations of the prevailing 'notice—consent' model, which serves as the basis for data subject empowerment. By legally emphasizing the fiduciary duty of the data trustee, the data trust mechanism facilitates elderly individuals—especially those with cognitive or informational barriers—in understanding the content and implications of privacy policies. In doing so, it elevates the role of elderly-related data principals and enhances the substantive protection of their rights and interests.

On the other hand, data trusts are particularly well-positioned to address the evidentiary difficulties encountered by elderly individuals in asserting data-related claims. Under the doctrinal logic of trust law, the trustee bears the burden of proving that fiduciary obligations have been fulfilled. Failure to meet this burden gives rise to the presumption of fault. Such a structure significantly shifts the burden of proof from data subjects towards trustees, thereby reducing the legal and procedural costs associated with seeking redress. In this way, data trusts both serve a preventive function and increase the likelihood of successful litigation outcomes for elderly-related data subjects.

Due to its capacity to represent individual interests and to collect and manage personal data in a rights-respecting manner, the data trust model has been recognised by international institutions. With the entry into force of the *Regulation (EU) 2022/868 on European Data Governance (the Data Governance Act)* on September 24, 2023, the data trust model received explicit legislative acknowledgment. The Act classifies 'data intermediation services'—which are functionally analogous to data trusts—as a distinct category, subjecting them to strict requirements of neutrality and fiduciary-like duties. This legislative framework aims to address structural shortcomings in the existing data protection regime and to harmonize the dual objectives of promoting data sharing and safeguarding individual

18 Liu Jieyong, *Data Trust for the Elderly: The Dilemma in the Utilization of Smart Pension Data and Its Countermeasures*, 1 Lanzhou Academic Journal 96, 96-99 (2024).

19 Zhai Zhiyong, *Data Trust: A New Solution for Data Governance*, 4 Oriental Law 61, 61-75 (2021).

privacy.

Drawing on the UK Open Data Institute's conception, a data trust refers to a mechanism in which data stewards manage data not for their benefit, but for the interest of defined beneficiaries. In parallel, the US notion of an 'information fiduciary' describes a person or entity that assumes a special duty of care for information acquired within a relational context. Based on these foundational ideas, scholars and practitioners have coalesced around a relatively narrow but widely accepted definition: a data trust is a legal structure designed to facilitate independent and fiduciary-based data stewardship.[20] On the basis of this definition, the present study explores the application of the data trust model to elderly-related data governance. Through examining pilot initiatives such as the UK Government Office for Artificial Intelligence's data trust trials and the 'Civic Data Trust' plan promoted by Sidewalk Labs, a Google-affiliated enterprise, it becomes evident that the US model of the information fiduciary may be of limited reference value in the Chinese context. The commercial orientation of private data controllers is difficult to reconcile with the higher fiduciary standards required for safeguarding elderly-related data subjects. Consequently, the inherent imbalance in the relationship between elderly individuals and data controllers is unlikely to be resolved within the US framework.

In contrast, the UK model—featuring independent third-party data trust institutions—offers more direct theoretical and practical guidance for China. Nevertheless, as a regulatory mechanism introduced from abroad, the application of the data trust in China faces considerable challenges, including ambiguity regarding data ownership and the legal framework for social utilisation of data.[21] According to the UK's report *Designing Decision Making Processes for Data Trusts: Lessons from Three Pilots*, the successful implementation of a data trust requires careful legal structuring tailored to specific application scenarios.

In light of the practical demands of elderly individuals and the unique characteristics of data use in the medical and eldercare sectors, the establishment of a public data trust may represent a viable institutional pathway. This mechanism would not only enhance the protection of elderly-related data rights but also promote the lawful and effective use of such data. Furthermore, it would support the development of intelligent eldercare services and the formation of a more secure, transparent, and inclusive

20 Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis Law Review 1183, 1183-1234 (2015).

21 Sun Hongchen, *The Dilemma and Outlet of Data Trust: Expediency or System Innovation*, 3 Business and Economic Law Review 116, 116-119 (2022).

data governance environment. In line with China's institutional conditions, the creation of a public data trust dedicated to elderly-related data in the healthcare and eldercare domains may constitute a constructive and context-sensitive attempt at systemic reform.

2. Conceptual Construction Grounded in Behavioural Control Theory. — Due to the limitations of traditional empowerment-based models, the imbalance of rights and obligations in the field of data circulation has remained unresolved. The preceding discussion on the decentralisation and socialisation of data ownership, and the data trust model that imposes fiduciary duties upon data controllers, offers a necessary theoretical basis for structural reform.[22] Specifically, the premise of informed consent underpins the legitimacy of data use, a fiduciary relationship is an essential condition between the data subject and the data controller, absolute control is a manifest feature of data relations, and the emergence of a dual ownership architecture is a necessary result of the evolving relationship between data controllers and data subjects. Based on this theoretical foundation, the present study draws upon behavioural control theory and the data trust model developed in the UK to conceptualise elderly-related data trust as a normative structure under trust law. Through the establishment of an intermediary layer between data subjects and data demanders, elderly individuals may delegate their data-related rights to professional and credible trustees. On the condition that the trustees strictly comply with the trust's stated purposes, they are required by law to perform their fiduciary duties—including the duties of loyalty and prudence—for the benefit of the data subjects. Trustees are expected to exercise data rights with full transparency, thereby ensuring that data is processed in a secure, lawful, and socially beneficial manner that safeguards the rights and interests of all parties involved.

The elderly-related data trust mechanism consists of four key actors: the trustor, the trustee, the beneficiary, and the data demander. Mainstream academic opinion defines the trustors as either the data controllers or a sufficient number of data subjects.[23] This formulation is intended to enhance the bargaining power of the trustor by increasing its control over the data, thus correcting the unequal distribution of rights and obligations between elderly-related data subjects and data controllers in the circulation process. However, the requirement for collective formation among data subjects is practically unfeasible in the context of eldercare, as elderly individuals

22 Feng Guo & Xue Yisa, *supra* note 10, 73, 73-76.

23 Yang Yingwu, *Data Trust: A New Path to the Legal Regulation of Data Transactions*, 25(S1) Journal of Southeast University (Philosophy and Social Science) 123, 124 (2023).

often lack the physical and cognitive capacity to spontaneously organise and negotiate with data trustees. Therefore, in order to ensure full protection of individual data rights, elderly-related data trustors may be defined as either data controllers or elderly persons with full civil capacity. For those who lack or possess limited civil capacity, legal guardians may act as trustors on their behalf. As to the problem of bargaining asymmetry, it should be addressed through enhanced government oversight in the selection of trustees and by providing preferential policy treatment. Within the legal framework of trust law, trustees are tasked with consolidating the rights of data subjects and using their professional expertise and institutional authority to balance the power of data controllers and data demanders.[24] In doing so, the trustee reshapes the power structure between data subjects and controllers and contributes to a more equitable configuration of rights and obligations.

The beneficiary in a data trust refers to the individual or entity entitled to the benefits derived from the trust. In the context of elderly-related data, this generally includes elderly individuals and their guardians, who are entitled to benefit from the value generated by the data. The trustor may also be a beneficiary and, in some cases, may be the sole beneficiary of the same trust. The trustee may also serve as a beneficiary, but may not be the sole beneficiary of the same trust. This structural arrangement ensures the trustee's incentive to act diligently while preventing conflicts of interest.

The institutional advantage of the data trust model lies in its capacity to exert dual constraints on the behaviour of data controllers through legal enforcement and incentive mechanisms. First, fiduciary duties, as codified in trust law, establish behavioural boundaries for trustees through the duties of loyalty and prudence. In accordance with article 25 of the *Trust Law of the People's Republic of China* (hereinafter referred to as the Trust Law), the trustee shall abide by the provisions in the trust documents and handle trust business for the best interests of the beneficiary. This requirement imposes direct constraints on any discretionary power exercised by data controllers in pursuit of profit maximisation.

Second, behavioural control theory emphasises the strong correlation between legal responsibility and behavioural consequences. This principle is reflected in the reversed burden of proof mechanism embedded in elderly-related data trust. In cases involving data leakage or abuse, the trustee must demonstrate that reasonable precautions were taken—such as data encryption, tiered access control, and other preventive measures. Failure to do

24 *Opinions of the Central Committee of the Communist Party of China and the State Council on Building Basic Systems for Data and Giving Full Play to the Role of Data Resources.*

so results in the application of presumed fault liability. This regulatory design compels trustees to proactively optimise their data management behaviour, thereby fostering an internally driven culture of preventive compliance.

At the legislative level, article 12 of the *Data Regulations of Shanghai* and article 4 of the *Regulations of Shenzhen Special Economic Zone on Data* both affirm the property rights and interests enjoyed by civil law subjects over data products and services derived from the lawful processing of data. At the policy level, documents issued by the CPC Central Committee and the State Council advocate for mechanisms through which individuals, enterprises, and public entities may share in the value and benefit generated from data.[25] These policy directives effectively recognise the property attributes of personal information.

In the academic community, there is a growing consensus on the property dimension of personal information. Professor *Lyu Bingbin* has argued for the legitimacy of protecting personal information as a property interest from the perspective of data circulation, suggesting that such protection better reflects individual autonomy and enhances data subject self-determination.[26] Professor *Xiang Qin* and Professor *Gao Fuping* suppose that personal information rights are essentially personality rights embedded with inherent property attributes.[27] Given the dual ownership structure that is characteristic of the trust model, the trustee holds legal title, while the beneficiary possesses equitable title and beneficial interest in the trust. Even without resolving the broader debate over data ownership, the property rights inherent in a data trust are clearly within the scope of rights protected under trust law.

C. Multi-Stakeholder Governance and Full-Chain Protection

1. Fiduciary Duties in Data Trusts. — At the level of data transmission and operation, the legal operation of data trusts must be clarified through the delineation of trustee powers and duties. First, trustees must strictly comply with the obligations established in the Trust Law, the *Implementation Measures for Administrative Licensing Matters of Trust Companies of the China Banking and Insurance Regulatory Commission*, and other relevant laws and regulations. Particular attention must be paid to the asymmetric

25 Cai Linan, *Data Trust Participates in Data Governance: Theoretical Logic and Implementation Mechanism*, 14(1) Chinese Review of Financial Studies 66, 66-75 (2022).

26 Lyu Bingbin, *The Path for Realizing Property Interests of Personal Information in the Context of Establishing the Data Property Rights*, 6 Journal of Comparative Law 67, 68 (2023).

27 Xiang Qin & Gao Fuping, *On the Property Attribute of Personal Information Rights and Interests*, 2 Nanjing Journal of Social Sciences 92, 92-100 (2022).

relationship between data subjects and trustees. Given the inherent vulnerability and relatively weak position of data subjects—especially elderly individuals—coupled with the institutional advantage held by trustees, fiduciary duties should be placed at the core of data trust governance. This normative arrangement serves to curb potential opportunistic or self-serving behaviour by trustees.

Accordingly, data controllers acting as trustees should bear the responsibilities of prudent and honest administration, managing entrusted data with integrity and in the best interests of the data subject. This framework promotes a balance between data utilisation and the rights of the data subject. The trustee's powers should include access control, audit oversight, and the handling of anonymised data. The trustee may select data management methods that best serve the principal's interests, including categorising data as static or dynamic. Static data may be limited in use through encryption keys or access tokens, while dynamic data may be subject to time-based usage rights that expire upon the conclusion of the authorised period, requiring renewal for continued access.

Second, the legal interests of trustees in relation to the data must be clearly defined. The *Opinions of the Central Committee of the Communist Party of China and the State Council on Building Basic Systems for Data and Giving Full Play to the Role of Data Resources*, adopted at the 26th meeting of the Central Committee for Deepening Overall Reform, propose a delineation of the lawful rights of participants in data generation, circulation, and use. This policy guidance suggests a pathway for establishing data property rights by generally recognising and protecting the proprietary interests held by data subjects, while allowing for phased and partial rights confirmation during the data lifecycle.

The lifecycle of data can be divided into two key stages: data acquisition and data monetisation. In the acquisition phase, elderly users may entrust their data to trust institutions, which are then authorised to enter into data use agreements with data demanders or processors on the principal's behalf, ensuring lawful and secure data handling. In the monetisation phase, processed and refined data products may be independently owned by the data demander or processor. Such entities would be entitled to manage and operate these data products and derive legitimate commercial value therefrom.

Third, trustees should bear both the burden of proof reversal obligation and the defect warranty obligation *vis-à-vis* data demanders. Where the principal initiates legal proceedings regarding breaches of trust, the principle of fault presumption may apply. The trustee must demonstrate that it has

fulfilled its fiduciary duties of loyalty, prudence and diligence, and has not engaged in conduct that conflicts with the interests of the data subject. The data subject, by contrast, is only required to prove the occurrence of harm. With respect to the trustee's obligations to the data demander, the doctrine of warranty against defects, as codified in the Civil Code, provides useful reference. As a strategic resource in the digital era, data has been recognised as one of the most valuable assets. Therefore, in promoting the circulation and productive reuse of data, data—when treated as a contractual subject matter—should not only fall within the ambit of general contract law but also be accorded special legislative protection applicable to data products.

Specifically, if the trustee delivers data that is defective—such as data sourced illegally or containing quality deficiencies—the data demander is entitled to demand corresponding legal remedies, regardless of whether such defects result in actual losses. Nonetheless, the data demander must also fulfil a reasonable inspection obligation within a defined period, consistent with general principles of contract law.

Furthermore, at the level of data service authorisation, the legal structure of data trusts must be supported by new legislative developments. This may include supplementary interpretations to the Trust Law that clearly recognise the full proprietary rights of data subjects over their original data. These rights should encompass data preservation, autonomous use, and self-directed commercialisation. At the same time, trust regulations should confirm that, under lawful and compliant conditions, trustees and data processors also hold legally recognised rights over derivative data that is produced through lawful processing activities. This dual recognition promotes both the protection of data subjects and the legitimate operation of data trust mechanisms within a stable legal framework.

2. Protection of Elderly-Related Data Under a Multi-Stakeholder Governance Mechanism. — The effective realisation of diversified governance in the field of elderly-related data protection requires the expansion of regulatory actors within a clearly defined scope, as well as the clarification of their respective legal duties and responsibilities. While governmental supervision remains the foundational pillar, the institutional framework must be extended to include meaningful participation by non-state actors.

On the one hand, the participation mechanism for public interest organisations should be systematised and strengthened. Given the relatively disadvantaged status of elderly individuals in digital environments, public interest organisations may serve as independent supervisory bodies conducting full-process compliance reviews of data collection, processing,

and circulation activities. Through such oversight, preferential protection for elderly-related data subjects can be achieved. Furthermore, public interest organisations should be formally integrated into the governance structure of the new integrated medical and elderly care service model. Under the guidance of the relevant provisions of the *Charity Law of the People's Republic of China* concerning privacy protection, these organisations may adopt oversight approaches analogous to service quality evaluation systems. Specifically, they may conduct follow-up surveys and feedback mechanisms targeting elderly users, thereby identifying and rectifying improper conduct in a timely manner.

On the other hand, the establishment of relevant industry associations should be both encouraged and institutionally supported. Such associations may specify, through their internal charters, the methods, procedures, and scope of data collection related to intelligent eldercare services. In the course of elderly-related data circulation, these associations may also provide normative recommendations to governmental bodies and public interest organisations, thereby enhancing regulatory adaptability and domain-specific standardisation.

In addition, the responsibilities of government actors within the integrated medical and elderly care model must be more precisely defined. First, in terms of governance participation, the government's leading role must be affirmed. On the basis of the *Government Procurement Law*, the essential legal elements governing data circulation—including conditions for data transactions, procurement procedures, and institutional structure—should be codified. Supplementary elements such as data collection protocols, data use parameters, and confidentiality standards should also be embedded into the overarching regulatory framework to ensure comprehensiveness and legal certainty.

Second, regarding data collection procedures, the current notification-based consent regime remains underdeveloped and functionally inadequate. In this respect, professionalised governmental review should serve as a substitute for individual self-auditing by elderly users. Data demanders may be permitted to obtain implied or general consent for data collection purposes, provided that the specific content and methods of collection receive formal approval by competent government departments. This approach may reduce procedural burdens on elderly individuals while preserving legality and oversight.

Third, with respect to data retention and retrieval, the state should enact laws and regulations specifying mandatory data retention periods for

elderly-related data. Furthermore, policy documents should designate specialised institutions within each administrative region to assume long-term custody and oversight responsibilities. These institutions should be staffed with dedicated personnel to ensure the integrity, security, and accessibility of elderly-related data throughout its lifecycle. Through such legal and institutional arrangements, the state can establish a unified data governance infrastructure that is capable of reconciling efficiency with rights protection in the field of smart eldercare services.

V. CONCLUSION

The regulation of elderly-related data represents a fundamental rule-of-law proposition in the digital era, aiming to reconcile the empowering potential of emerging technologies with the imperative of rights protection. It also serves as a crucial foundation for safeguarding the lawful rights and interests of elderly individuals and enhancing the overall quality of eldercare services.

Looking ahead, the regulatory framework governing elderly-related data is expected to become more systematic and refined. With the continuous advancement of information technologies and the progressive expansion of their application in eldercare contexts, the processes of data collection, management, and utilisation will evolve toward greater efficiency and precision. Under the integrated model of medical and elderly care services, improvements in data infrastructure will ensure the comprehensiveness and accuracy of elderly-related data. At the same time, enhanced capabilities in data analysis and algorithmic processing will enable the delivery of more personalised, responsive, and targeted eldercare services.

Nevertheless, a number of legal and technical challenges must be addressed in this process. These include issues concerning the protection of personal privacy, the mitigation of cybersecurity risks, and the appropriate balancing of data sharing with lawful and proportionate utilisation. Each of these issues demands sustained legal attention and institutional response.

Accordingly, there is an urgent need to strengthen the legislative and regulatory architecture for elderly-related data. This entails refining existing legal norms, establishing a robust data protection mechanism, and enhancing institutional capacity for data security oversight. Only by ensuring that elderly-related data is processed and utilised within a lawful, secure, and transparent framework can its full social and public value be realised.

The exploration of regulatory pathways for elderly-related data within integrated medical and elderly care services constitutes a long-term and

complex task. It requires continued attention to the evolving nature of elderly-related data ecosystems and responsiveness to emerging social and technological demands. Regulatory strategies must be continuously adapted and optimised to enhance effectiveness. Ultimately, sustained academic and policy efforts are necessary to support the development of a more comprehensive, efficient, and secure smart eldercare system that is capable of meeting the multidimensional needs of an ageing society.

(Edited by Gong Li)

新型医养结合模式下涉老数据流通规制路径研究

内容提要 在新型医养结合养老服务中，涉老数据因其多维性与敏感性，叠加数据主体的脆弱性与依赖性，呈现出公私法交融的复杂权益特征。当前涉老数据流通存在法律规范之间衔接不畅、数据权属虚化以及相关部门监管不足等问题。对此，应从数据服务授权、数据传输运行与数据监督保障三个层次审视多元主体之间法律关系，建构以“自上而下协调既有规范、自下而上引入数据信托”的双轨制实现路径与“政府—社会公益组织—行业协会”的全链式规制主体为核心内容的涉老数据流通规制体系，以期维护数字弱势群体权益。