How Do Flexible Norms Achieve Effectiveness for Sensitive Personal Information Governance in Tourism Big Data Commercialization?

This study investigates how flexible norms achieve de facto binding force in governing sensitive personal information within tourism big data commercialization, addressing the theoretical gap regarding their effectiveness mechanisms in the absence of state coercion. Employing W. Richard Scott's Three Pillars of Institutions (regulative, normative, cultural-cognitive) as a theoretical framework, this research conducts a comparative case analysis of 12 representative flexible norms, including national guidelines, industry standards, corporate policies, and self-regulatory covenants. Flexible norms generate effectiveness through three synergistic mechanisms: (1) role-driven mechanisms that clarify governance subjects and accountability structures; (2) content-driven mechanisms that translate abstract principles into operational rules through detailed institutional design; and (3) enforcement-driven mechanisms that leverage public commitments, training systems, and reputational constraints to promote norm internalization. This study moves beyond static textual analysis to reveal the dynamic mechanisms through which flexible norms achieve practical effectiveness, offering a systematic theoretical explanation grounded in organizational institutionalism and providing actionable pathways for sensitive information governance in data-driven tourism contexts.

Keywords: *Tourism Big Data; Flexible Norms; Sensitive Personal Information; Effectiveness*

Introduction

Research Background and Problem Statement

Driven by the wave of digital transformation, the tourism industry has emerged as a critical domain for the data-driven economy. The entire life-cycle of tourism activities—from pre-trip information search and itinerary planning, to booking tickets, accommodation, and dining, to transportation navigation during the trip, and finally to post-trip evaluations and sharing—continuously generates massive data footprints (Safaa, Oruezabala, & Bidan, 2021; Benhaida, Safaa, & Perkumienė, 2024). This data encompasses not only basic identity information but also highly sensitive data, such as location trajectories, biometric information, payment records, and personal preferences, collectively constituting what is termed "tourism big data" (Perkumienė, 2025; Florido-Benítez, 2024).

The commercial utilization of tourism big data creates immense economic value. Through precise user profiling and personalized recommendations, entities such as online travel agencies (OTAs), hotel groups, and airlines can optimize services, enhance customer experiences, and implement targeted marketing (Buhalis, Leung, & Lin, 2023). However, this value-creation process is

accompanied by systemic privacy risks. Within the multi-actor, long-chain circulation network of tourism services, tourists' sensitive personal information frequently flows and is shared among consumers, platforms, suppliers, third-party service providers, and technology vendors, forming a complex data ecosystem (Yallop et al., 2023). Each instance of data transfer can potentially become a point of leakage. Whether due to cyberattacks, internal policy violations, or partners' security lapses, large-scale data breaches remain a persistent threat (Herke, Tóth, & Perkumienė, 2025). This coexistence of "value creation" and "privacy risk" constitutes the fundamental paradox of tourism big data commercialization (O'Connor, 2020).

In response to the systemic risks mentioned above, traditional governance paths have primarily relied on rigid norms backed by state coercive power, such as various countries' Personal Information Protection Laws and related data security regulations. These laws and regulations set baseline standards for data collection, processing, storage, and transmission. However, when confronted with rapidly evolving tourism technologies and dynamic, complex commercial scenarios, rigid regulation faces a significant "pacing problem" (Marchant, 2011). The complexity and lengthy nature of legislative processes stand in stark contrast to the exponential iteration speed of tourism technology, leading to what is known as the "Collingridge Dilemma" (Collingridge, 1980). In the early stages of technological development, regulatory intervention is difficult due to insufficient risk information. Conversely, when a technology's social impacts become clear and demand regulation, its developmental path and application models have often become highly solidified, making regulatory adjustment extremely costly. Within the domain of tourism big data governance, this dilemma manifests in two ways: laws related to tourism may be outdated regarding the technological landscape they address by the time they are enacted, or conversely, they may inadvertently spur the creation of new pathways for regulatory circumvention (Moses, 2007; Zhang, 2023). Furthermore, tourism services involve numerous heterogeneous actors—OTAs, hotels, airlines, local operators, payment processors, etc.—forming a loosely coupled complex network. Traditional "command-and-control" regulatory models struggle to penetrate these multi-layered outsourcing and partnership arrangements to effectively monitor and enforce data governance across the entire data life-cycle. This results in high compliance costs and significant enforcement difficulties (Kalesnykas, 2025).

Consequently, a flexible governance path has gradually emerged and plays an increasingly important role in practice. This refers to flexible norms represented by industry guidelines, technical standards, corporate codes of conduct, privacy certifications, and self-regulatory conventions (Luo & Song, 2009; Shen, 2023). Flexible norms are a normative model rooted in the concepts of agile and flexible governance. Originating from the idea of flexible governance, it does not rely on top-down administrative compulsion but rather employs "non-mandatory methods to stimulate the inner potential, initiative, and creativity of governance partners and objects" to achieve good governance goals (Tan, 2014). Compared to rigid norms, which directly define the rights and obligations of regulated subjects and enforces provisions through coercive measures, flexible norms recognize informal relationships as an important feature of social relations. It transmits pressure through

these informal relationships to mitigate conflicts and contradictions in a non-violent, low-coercion manner (Wu & Hu, 2021). Participants in flexible governance manage internal affairs through non-mandatory means such as rational communication and collaborative cooperation, reaching consensus through equal dialogue. Unlike rigid norms, which are formulated by the state and enforced by coercive power, flexible norms are typically developed jointly by industry organizations, corporate alliances, or multi-stakeholder groups. The binding force does not stem from external sanctions but relies on the voluntary compliance of participants (Shelton, 2000; Abbott & Snidal, 2000). In tourism big data governance, elements such as big data guidelines from government-affiliated platforms, travel data standards from industry associations, privacy policies and developer agreements formulated by major OTAs, and various privacy protection certifications collectively constitute a flexible governance system.

However, flexible norms are not without their own dilemmas. On one hand, flexible norms shall maintain its flexibility and therefore cannot use mandatory clauses like rigid norms to directly constrain behavior. On the other hand, flexible norms' reliance on participants' voluntariness raises a critical question: in the absence of state coercive power, how can the effectiveness of flexible norms be ensured?

This study aims to delve into the underlying mechanisms through which flexible norms function in the governance of sensitive personal information within tourism big data. In the absence of coercive enforcement, what specific mechanisms enable flexible norms to effectively constrain participants and thus play a role in governing sensitive personal information in tourism big data?

Current Research Status on Flexible Governance

Recognizing the limitations of rigid norms, academia has increasingly turned its attention to flexible governance models centered on flexible norms (Tan, 2014). In international law, "soft law" was initially defined as normative instruments that are "not legally binding in principle, but may produce practical effects" (Shelton, 2000; Abbott & Snidal, 2000). Subsequently, this concept was introduced into domestic law, particularly in emerging fields like technology governance and environmental governance, referring to rules, principles, and codes of conduct formulated by non-state actors and implemented through non-coercive means (Shen, 2023). Researchers generally agree that flexible norms offer advantages such as flexible formulation processes, rapid responsiveness, and the ability to incorporate diverse participants, enabling better adaptation to technological iteration and social change (Luo & Song, 2009).

In the field of technology governance, significant research has accumulated on the analysis of flexible norms texts, such as AI ethics guidelines (Jobin, Ienca, & Vayena, 2019) and data privacy protection frameworks (Zeng, Liang, & Zhang, 2024). Scholars have outlined the core principles of these texts and compared different global governance models (Gutierrez, Marchant, & Tournas, 2020).

However, current research exhibits a significant theoretical gap: numerous studies remain at the static analysis of normative texts—describing and comparing

"what flexible norms say"—while critically lacking dynamic mechanism inquiries into "how flexible norms produce actual effects" (Bietti, 2020). Although some scholars suggest that flexible norms may exert influence through mechanisms like reputation, market pressure, or community identity, these assertions are mostly empirical observations lacking a systematic theoretical framework to explain how this "de facto binding force" is generated, maintained, and operates. Regarding its effectiveness in the high-risk area of sensitive personal information governance, in-depth theoretical and empirical research is particularly scarce.

Research Purpose

To fill the aforementioned theoretical gap, this study proposes introducing the new institutionalism theory of organizational sociology. Based on W. Richard Scott's "Three Pillars of Institutions" framework (Scott, 2014), this study aims to explain the sources of flexible norms' effectiveness and its driving mechanisms. Scott argues that institutions are social structures composed of three major elements—regulative, normative, and cultural-cognitive—which together provide stability and meaning to social life.

The regulative pillar emphasizes explicit rule-setting, monitoring, and sanctioning activities, with its core mechanism being coercion and fear of violating rules. This is the typical domain where rigid norms operate. (Scott, 2014).

The normative pillar emphasizes obligations, expectations, and appropriateness in social life. (March & Olsen, 1989) It guides actors to fulfill responsibilities commensurate with their social roles through value assessment and normative constraints. Flexible norms, such as industry self-regulatory conventions and professional certifications, primarily operates at this level.

The cultural-cognitive pillar focuses on the shared understandings, cognitive frameworks, and beliefs that actors hold regarding specific situations and modes of behavior (Suchman, 1995). When a set of rules is internalized as the "taken-for-granted" way of doing things, its binding force is most profound. For example, viewing user privacy protection as a moral baseline that entity "shall" uphold, rather than merely a compliance requirement.

Specifically applied to tourism big data governance, an effective set of flexible norms need not only to establish a consensus at the normative level that "protecting user privacy is industry best practice," but also to provide actors with a predictable action framework through clear rules, role definitions, and implementation mechanisms. Ultimately, it needs to shape the relevant actors' value identification with data protection. The Three Pillars framework will help us deeply understand how flexible norms function, ultimately achieving the transformation from "what ought to be" rules to "what is" action. This study will select typical data governance flexible norms within the tourism industry as research objects, deeply analyzing their institutional designs across the regulative, normative, and cultural-cognitive dimensions, and examining how these designs collectively produce "de facto binding force" on participating entities.

Methodology

Theoretical Framework: W. Richard Scott's Three Pillars of Institutions

Scott defines institutions as "composed of regulative, normative, and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life" (Scott, 2014, p. 56). This framework moves beyond a legal-centric perspective that emphasizes state coercive power, offering a systematic analytical tool for understanding how flexible norms generates de facto binding force.

The regulative pillar focuses on the coercive binding force of institutions. Its core mechanism is instrumental "expediency," achieving behavioral regulation through explicit rule-setting, monitoring, and sanctions (Scott, 2014). The legitimacy basis of this constraint lies in "regulative legitimacy"—where actors comply with rules due to fear of sanctions (Suchman, 1995). Although the flexible norms at the center of this study do not possess the coercive power of national laws, they still contain unique reward and punishment logics implemented internally by enforcement entities. For example, industry association standards may impose internal sanctions through means such as revoking certification qualifications or expelling members; corporate self-regulatory conventions may create constraints through intra-industry notifications or membership revocation. Therefore, proceeding from the regulative pillar, this study will focus on examining the internal reward and punishment mechanisms and role-driven implementation structures embodied in the texts.

The normative pillar concerns the obligatory and expectational dimensions of social life. It includes "the specification of goals or objectives" and "the appropriate ways to pursue them" (Scott, 2014, p. 64). Its legitimacy basis lies in "normative legitimacy"—where actors comply with rules due to recognition of social obligations (Suchman, 1995). The core of the normative system is the "logic of appropriateness," where actors act based on their understanding of their roles and obligations (March & Olsen, 1989). In the realm of flexible norms, this pillar manifests through the formulation of standards, certification implementation, guideline issuance, and other means that specify what constitutes normatively compliant behavior.

The cultural-cognitive pillar is the most sociologically oriented part of Scott's theory, emphasizing that institutions are "composed of shared conceptions that constitute the nature of social reality and the frames through which meaning is made" (Scott, 2014, p. 67). Its legitimacy basis lies in "cognitive legitimacy"—where actors comply with rules because they view them as "taken for granted" (Suchman, 1995). The core mechanism of cultural-cognitive elements is "orthodoxy," where actors follow a certain behavioral pattern because it is considered the taken-for-granted way of doing things, as "the way we do things in these situations" (DiMaggio & Powell, 1991). For Flexible norms, their effectiveness ultimately depends on whether it can be internalized by relevant actors as a shared belief and behavioral logic, gradually making compliant behavior the "natural choice" for participants through public commitments, information

disclosure, performance indicators, and other means.

In the subsequent analysis, this paper will categorize the governance designs distributed across the 12 samples into the "regulative," "normative," and "cultural-cognitive" domains. It will then examine which specific effectiveness-guaranteeing mechanisms emerge under each pillar, thereby systematically revealing the mechanisms through which flexible norms generate effectiveness under the Three Pillars of Institutions framework. This framework echoes the analysis of institutional change and organizational fields by Greenwood et al. (2008) and provides a foundation for subsequent theoretical construction.

Research Design: Comparative Case Analysis

This study adopts comparative case analysis as its core research design. Comparative case analysis, through the systematic comparison of a small number of carefully selected cases, reveals the key mechanisms and combinations of conditions leading to specific outcomes. It is particularly suitable for exploring "how" and "why" causal process questions (George & Bennett, 2005; Yin, 2018). The core question of this study—"how do flexible norms generate effectiveness"—is fundamentally a question of mechanism explanation. Comparative case analysis allows for tracing the entire chain from norm formulation to implementation, capturing the specific operational circumstances of the Three Pillars in practice.

Sample Selection

This study employs purposive sampling, selecting 12 representative flexible norms. Sample selection follows the principle of "maximum variation sampling," aiming to cover flexible norms with different formulating bodies, different application domains, and different forms to ensure the richness and explanatory power of the research findings (Patton, 2015). According to the typology of case selection by Seawright and Gerring (2008), this study's strategy can be classified as selecting "diverse cases"—selecting representative cases within the value range of the independent variable (norm type) to maximize observed differences.

Specifically, sample selection considered three key dimensions:

1.

(1) Formulating body: Including national ministries, provincial standardization bodies, industry associations, and corporations;

(2) Norm level: Including national/provincial guidelines, industry standards, corporate policies, and self-regulatory conventions;

(3) Binding intensity: Forming a continuum from "certification standards" to "voluntary commitments." Through the cross-combination of these three dimensions, the 12 samples cover the main types of flexible norms currently existing in China. The specific composition of the samples is as follows: (see Table 1)

Table 1. *Basic Information on the 12 Flexible Norm Samples*

No.	Category	Sample Name	Issuing Body	Year	Description
1	National/Provincial Government Industry Guidelines or Standards	Tourism Big Data Security and Privacy Protection Requirements (Draft for Comments)	Ministry of Culture and Tourism	2026	An industry guidance document issued by a national ministry, reflecting top-level regulatory intent.
2		GB/T 35273-2020 Information Security Technology - Personal Information Security Specification	State Administration for Market Regulation	2020	A national recommended standard specifying the relevant behaviors of personal information controllers in various stages of information processing.
3		DB62/T 5083-2025 Tourism Big Data Security and Privacy Protection Standard	Gansu Provincial Market Supervision Administration	2025	A local standardization document, reflecting regional governance characteristics.
4		DB14/T 3539-2025 Guide to Privacy Protection in Tourist Hotel Guest Rooms	Shanxi Provincial Market Supervision Administration	2025	A privacy protection guide for a specific scenario, reflecting vertical domain

No.	Category	Sample Name	Issuing Body	Year	Description
5	Industry Association Standards	T/CSAS 0016-2025 Requirements on personal information protection	Sichuan Cyberspace Security Association	2025	Security standards formulated by an industry association, emphasizing technical compliance.
6		T/NBSIA 003-2024 Data privacy protection and security requirements for urban public transportation users	Ningbo Software Industry Association	2024	Focuses on public transportation data privacy, including technical requirements such as anonymization.
7		T/CCTAS 11-2020 Self-discipline specifications for app-based ride-hailing company safety and security operation	China Communications and Transportation Association	2020	An industry self-regulatory norm for ride-hailing, covering safe operation and data protection.
8		Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)	Internet Society of China	2025	Focuses on personal information protection in apps, with a broad scope of application.
9	Corporate Privacy Policies	F's Rules on the Protection of	F corporation	2025	An online travel

No.	Category	Sample Name	Issuing Body	Year	Description
	& Industry Self-Regulatory Covenants	Minors' Personal Information			platform's special protection rules for minors' personal information.
10		F's Privacy Policy	F corporation	2025	The platform's overall privacy protection rules.
11		X's Personal Information Protection Policy for Driver/Guide End	X corporation	2025	The platform's personal information protection rules for the driver
12		Self-Regulatory Covenant for Promoting Interconnectivity and Interoperability of Internet Platforms	Internet Society of China	2026	A multi-party self-regulatory covenant aimed at promoting data interconnectivity and interoperability between platforms.

The above samples constitute a multi-level flexible norms sample library, encompassing public norms from central to local levels, technical standards formulated by industry associations, and corporate privacy policies directly targeting users. This layered design facilitates examining the performance differences of norms with different sources of authority and varying binding intensities under the Three Pillars framework.

Analytical Strategy: Thematic Analysis and Mechanism Identification

This study, according to W. Richard Scott's Three Pillars of Institutions, performs a higher-level abstraction of mechanisms operating in different directions, summarizing them into three core categories: (see Table 2)

Table 2. *Key Operational Elements*

Dominant Pillar	Core Question	Key Operational Elements
Regulative	Expediency	Clear designation of enforcement actors, internal reward/punishment systems, supervision and accountability mechanisms
Normative	Appropriateness	Refinement of concepts, contextualization of rules, clarification of responsibilities
Cultural-Cognitive	Conceptions	Public commitment, internalization through training, reputation constraints, pressure transmission

Paired comparison and the method of difference will be employed, contrasting similarities and differences in key dimensions between effective and ineffective cases to summarize universal mechanisms. The comparison logic adopts a "most similar cases design" or "most different cases design," controlling for extraneous variables and focusing on key conditions (George & Bennett, 2005). Through multiple sets of comparisons, core mechanisms will be distilled, ultimately forming a theoretical explanation of the generative logic of flexible norms effectiveness. Through this analytical strategy, this study aims to systematically depict the comprehensive picture of how flexible norms construct effectiveness under the Three Pillars of Institutions, and ultimately abstract a cross-case common mechanism model, thereby better understanding the operational logic of flexible norms in the governance of sensitive personal information.

Analysis: A Comparative Case Study Based on 12 Samples

Analytical Framework: Representative Design Elements of the Three Pillars of Institutions

(a) Regulative

The regulative dimension primarily examines whether a document can form effective constraints on the regulated objects through clear responsible subjects and institutional design. The executing subject is the starting point of regulation; only by clarifying "who is responsible" can the subsequent implementation and execution of the system be ensured. Internal execution systems are the carriers of regulation, including safety management, risk assessment, emergency response, compliance audits, and other institutional designs, reflecting the systematization and completeness of regulation.

(b) Normative

The normative dimension focuses on the degree of rigor and operability of the document itself. Clear concept definition is the foundation of normativity; only with clear terminology and defined boundaries can ambiguity in understanding and implementation be avoided. Detailed institutional design is the core of normativity. Documents need to systematically stipulate various requirements according to business logic or the data life-cycle, such as specific operational norms for collection, storage, use, sharing, deletion, and other stages. Additionally, a complete normative document should include specific responsibility clauses, covering the division of obligations for different subjects in different scenarios, responsibility constraints for third-party cooperation, and disposal measures after violations, ensuring that every requirement has a clear responsibility attribution and accountability basis. These three types of elements are selected because they reflect the degree of transformation of a document from "abstract principles" to "enforceable rules."

(c) Cultural-Cognitive

The cultural-cognitive dimension examines whether a document can promote the internalization of compliance awareness and the formation of organizational culture through external commitments and internal education. Public commitment is the external manifestation of the cultural-cognitive aspect, including publicizing complaint channels, disclosing algorithm principles, etc., reflecting the organization's respect for users' right to know and choose, and forming the basis for building trust. Training systems are the internal guarantee of the cultural-cognitive aspect, ensuring the formation of inherent compliance motivation by incorporating compliance requirements into new employee induction, management promotion, and annual training for all staff. Social reputation is the outcome feedback of the cultural-cognitive aspect, including methods like self-discipline compliance evaluation, signing industry conventions, and publicizing violative behaviors, forming external supervision and reputational constraint mechanisms. These three types of elements constitute a cultural-cognitive system of "building external trust + cultivating internal awareness + accepting social supervision."

Textual Comparative Analysis: Main Mechanisms in 12 Flexible Norms

Based on the texts of the 12 samples, the measures adopted by flexible norms summarized according to the framework of representative design elements of the three pillars of institutions, as follows. (see Table 3)

Table 3. *Measures in 12 Flexible Norms*

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
1	Tourism Big Data Security and Privacy Protection Requirements (Draft for Comments)	**Implementing Entities:** Tourism big data management institutions, tourism enterprises, consumers, research departments. **Internal Systems:** Requires the establishment of security management system, data security risk assessment plans, data usage assessment systems, data retirement strategies, etc.	**Concept Definitions:** Defines core terms such as "tourism big data," "tourists' personal sensitive information," "tourism information collection devices," "tourism mobile applications," and "data retirement." **System Design:** Classifies data into 5 levels and proposes detailed security requirements, also covering operations, maintenance, and monitoring management. **Responsibility Clauses:** Specifies security responsibilities and obligations for different entities like "tourism big data management institutions," "tourism enterprises," "tourists," and "tourism research departments" in	**Public Commitment:** Requires tourism mobile app publishers to formulate a privacy policy and inform users of the rules for collecting and using personal information. **Training System:** No explicit mention of employee training systems, but requirements for relevant personnel's capabilities are implied in personnel security management. **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			corresponding sections.	
2	GB/T 35273-2020 Information Security Technology - Personal Information Security Specification	**Implementing Entities:** Personal information controllers, with the legal representative bearing overall responsibility; large-scale processors shall appoint a dedicated protection officer. **Internal Systems:** Requires the establishment of systems for security impact assessments, complaint management, security incident emergency plans, and records of processing activities.	**Concept Definitions:** Defines over 30 key terms like personal information, sensitive personal information, user profiling, de-identification, and anonymization in detail, supplemented by informative appendices. **System Design:** Systematically stipulates the full-process specifications from collection, storage, use, entrusted processing, sharing/transfer to public disclosure, and elaborates on the rights of personal information subjects. **Responsibility Clauses:** Details the division of responsibilities and obligations between the controller and third parties in	**Public Commitment:** Mandates the formulation and public release of a personal information protection policy to clearly inform users of processing rules. **Training System:** Explicitly requires regular specialized training and assessment on personal information security for personnel in personal information processing roles. **Social Reputation:** As a fundamental national standard, compliance with this standard is a significant mark of commitment to personal information protection, helping to build and maintain a positive image among users and the public.

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			aspects such as entrusted processing, sharing, transfer, and third-party access management.	
3	DB62/T 5083-2025 Tourism Big Data Security and Privacy Protection Standard	**Implementing Entities:** Owners of tourism big data (platform/system user units, tourism service enterprises). **Internal Systems:** Requires the formulation of detailed data classification and grading rules, data full life-cycle security management systems, and the establishment of approval processes for data provision and disclosure, data usage systems, and data retirement procedures.	**Concept Definitions:** Defines terms such as "tourism big data," "tourists' personal sensitive information," "tourism big data owners," and "data retirement." **System Design:** Classifies data into 5 levels and defines levels, usage scope, and examples in a table format; proposes detailed security measures, covering operations, maintenance, and monitoring management. **Responsibility Clauses:** Proposes specific responsibilities and obligations for cross-institutional collection, data applicants, and data users in	**Public Commitment:** Requires formulating a data provision and disclosure strategy, clarifying purpose, scope, conditions, and limitations, and displaying a data resource catalog. **Training System:** Mentions in operations management "regularly organizing emergency drills and personnel training to enhance comprehensive response capabilities for data security and privacy protection incidents" . **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			aspects such as data collection, provision/disclosure, and use/processing.	
4	DB14/T 3539-2025 Guide to Privacy Protection in Tourist Hotel Guest Rooms	**Implementing Entities:** N/A **Internal Systems:** Requires the establishment of internal management and supervision mechanisms, employee privacy protection training systems, visitor management systems, systems for signing privacy protection clauses with suppliers, and emergency response plans.	**Concept Definitions:** Defines "tourism hotel" and "guest room privacy." **System Design:** Provides specific, actionable guidance from six aspects: basic principles, facilities and equipment, information security, organizational management, emergency response, and complaints and supervision. **Responsibility Clauses:** N/A	**Public Commitment:** Recommends that hotels publicize their privacy protection policies and complaint channels. **Training System:** Explicitly requires "regular privacy protection training for employees to enhance their awareness and ability to protect guest privacy" , and stipulates that training content includes behavioral norms for cleaning and maintenance personnel. **Social Reputation:** N/A
5	T/CSAS 0016-2025 Requirements on Personal Information Protection	**Implementing Entities:** Personal information processors, requiring the legal representative to bear overall responsibility, and establishing	**Concept Definitions:** Defines over 30 terms such as personal information, sensitive personal information, automated decision-making, cross-border	**Public Commitment:** Requires formulating and publicly disclosing personal information processing rules, prompting users to read them via pop-up windows when the app is first launched.

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
		a dedicated personal information protection officer and working body. **Internal Systems:** Requires establishing a comprehensive system including personal information protection regulations, classification and grading management.	transfer, and separate consent, aligning with national standards like GB/T 35273. **System Design:** Covers the full life-cycle, and proposes special security requirements for scenarios like joint processing, entrusted processing, automated decision-making, cross-border transfer, and region-specific contexts. **Responsibility Clauses:** Clearly defines the specific obligations of personal information processors in different scenarios, such as obtaining separate consent, conducting impact assessments, signing contracts, maintaining records, supervising third parties, and	**Training System:** Includes a dedicated chapter, Chapter 12 "Personnel Management and Training," requiring background checks for key position personnel, signing personal information protection agreements, and providing education and training for employees who may access personal information. **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			stipulates joint liability.	
6	T/NBSIA 003-2024 Data Privacy Protection and Security Requirements for Urban Public Transportation Users	**Implementing Entities:** Urban public transport operators. **Internal Systems:** Emphasizes adhering to legal, legitimate, and necessary principles for collecting and using data, adopting technical and managerial measures to prevent leakage, tampering, or misuse.	**Concept Definitions:** Defines highly technical terms such as "user behavior data," "anonymous identity authentication," "unlinkable traceability," "zero-knowledge proof," "C-L signature," and "K-times anonymous technology." **System Design:** Centers around three core goals: anonymous identity authentication, unlinkable traceability, and data collaboration. It designs a full-process technical implementation scheme from registration, payment to authentication, providing specific algorithm formulas and flow charts.	**Public Commitment:** Requires informing users of data collection purposes and obtaining consent, and providing a privacy policy. **Training System:** No explicit mention of employee training, but technical requirements imply a need for technical competence of operating personnel. **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			Responsibility Clauses: N/A	
7	T/CCTAS 11-2020 Self-discipline Specifications for App-based Ride-hailing Company Safety and Security Operation	**Implementing Entities:** Ride-hailing platform companies, requiring the establishment of a safety management committee, dedicated safety management organization, and safety emergency team. **Internal Systems:** Requires establishing 12 systems including safety production responsibility, objective management, regular meetings, archives, training, driver/vehicle management, emergency plans, hazard investigation, rewards/punishments, and annual review and revision.	**Concept Definitions:** Defines ride-hailing specific terms like "trip sharing," "phone number protection," "accumulated service duration," and "complaint suspension." **System Design:** Forms a closed loop from safety assurance, safety functions/equipment, driver/vehicle management, operational management, network information security management, complaints/emergencies, hazard risks, performance management to compliance evaluation. **Responsibility Clauses:** Clearly defines the platform's safety management responsibility for drivers and	**Public Commitment:** Requires clarifying rights and responsibilities of all parties through electronic agreements, and obtaining explicit user consent before collecting information. **Training System:** Requires "timely promotion and training on safety management systems" , integrating safety training into the safety management system construction. **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			vehicles, requires purchasing carrier liability insurance, ensuring the security of prepaid funds, and signing agreements with banks/payment institutions.	
8	Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)	**Implementing Entities:** Mobile internet application service providers, requiring the establishment of a compliance management organizational structure. **Internal Systems:** Requires establishing a four-level system of "policies, management regulations, operational rules, forms and templates," including operational mechanisms for compliance risk assessment, risk response, compliance audits, and	**Concept Definitions:** Clarifies core concepts such as "user rights protection compliance," "compliance risk," and "compliance management." **System Design:** Systematically outlines six key compliance areas: service provision, personal information protection, algorithmic recommendation, service fees, user complaint handling, and customer service hotlines, listing specific compliance requirements for each. **Responsibility Clauses:** Details	**Public Commitment:** Requires formulating and publicly disclosing personal information processing rules, and encourages proactively disclosing compliance audit results in CSR reports. **Training System:** Includes a dedicated section "Organizing User Rights Protection Compliance Training," requiring establishing a normalized compliance training mechanism, integrating user rights protection into new employee orientation, management promotion training, and annual training, establishing training records, and evaluating effectiveness. **Social Reputation:** By

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
		compliance rectification.	the specific responsibilities of the board, compliance officer, compliance coordinators, and business departments, and proposes differentiated compliance management requirements for apps, SDKs, distribution platforms, and smart terminals.	establishing a sound compliance management system, conducting compliance training, and accepting external supervision, it aims to enhance user trust, internalize compliance as corporate culture, and enhance market competitiveness.
9	F's Rules on the Protection of Minors' Personal Information	**Implementing Entities:** service provider (platform operator). **Internal Systems:** Requires establishing internal management mechanisms for the protection of minors' personal information, including access authority control, principle of minimum necessary authorization, staff behavior	**Concept Definitions:** Clarifies the definition of "minor" (under eighteen years old) and distinguishes "children" (under fourteen years old). **System Design:** Specifically for minor scenarios, stipulates basic principles for collection and use, separate consent mechanisms (guardian's separate consent for children under fourteen), special	**Public Commitment:** Specially formulates and publicly releases minor protection rules, prompting guardians to read and understand them. **Training System:** N/A **Social Reputation:** N/A

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
		records and control, and emergency response plans.	protection measures for information sharing/transfer, storage period and location, and security protection measures. **Responsibility Clauses:** Clarifies the responsibilities of guardians, the platform's responsibilities, and the obligations of third-party partners (prohibition of sub-entrustment, assisting in responding to rights requests, etc.).	
10	F's Privacy Policy	**Implementing Entities:** service provider (platform operator). **Internal Systems:** Requires establishing a data security management system, including organizational structure, system design, personnel management.	**Concept Definitions:** Defines terms such as affiliates, personal information, sensitive personal information, children, personal information deletion, device information, service log information, de-identification, and anonymization. **System Design:** Covers	**Public Commitment:** Formulates and publicly releases a privacy policy, prompting users to read and understand it. **Training System:** Explicitly mentions "We will hold security and privacy protection training courses to enhance employees' awareness of the importance of protecting personal

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			the full process: information collection and use, partners and transfer/disclosure, information storage, user rights, minor protection, and policy updates. **Responsibility Clauses:** Clarifies the platform's responsibilities as the personal information controller, including notification and consent, security assurance, responding to rights requests, and security incident handling; constrains partner responsibilities through agreements.	information." **Social Reputation:** N/A
11	X's Personal Information Protection Policy for Driver/Guide End	**Implementing Entities:** Operator of the App. **Internal Systems:** Requires establishing an information security assurance system, having obtained	**Concept Definitions:** Defines terms such as personal information, sensitive personal information, personal information deletion, children, and minors.	**Public Commitment:** Formulates and publicly releases a personal information protection policy, prompting users to read and understand it. **Training System:** Explicitly mentions "regularly

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
		ISO27001 and PCI-DSS certifications; strictly monitors employees who may access information, requires them to sign confidentiality agreements, and conducts regular training; establishes approval mechanisms for important operations like data access, transmission, and desensitization.	**System Design:** Covers specific business scenarios like account registration and management, business cooperation and order management, financial settlement, customer communication, security assurance, customer service, course training, and permission access. **Responsibility Clauses:** Clarifies the platform's responsibility for collecting and using user information, security assurance responsibility, and responsibility for responding to user rights requests; constrains partner responsibilities through agreements.	conducting information security training for employees, requiring them to form good operating habits in daily work and enhance data protection awareness." **Social Reputation:** N/A
12	Self-Regulatory Covenant for	**Implementing Entities:** Internet platform operators; the	**Concept Definitions:** Defines the concepts of "internet platform"	**Public Commitment:** Signing the Convention signifies a public

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
	Promoting Interconnectivity and Interoperability of Internet Platforms	Internet Society of China acts as the implementing agency responsible for organization and execution. **Internal Systems:** Requires signatory units to establish and improve data security management systems, strengthen the application of security technical means such as data encryption and access control, and formulate data security incident emergency plans.	and "interconnection and interoperability." **System Design:** Gradually carries out application and service interconnection and interoperability, external link identification and access, and data interconnection and interoperability in phases; requires formulating fair and open data management rules, following the principle of minimum necessity; requires setting up convenient user complaint and feedback channels. **Responsibility Clauses:** Clarifies that platform operators shall comply with laws and regulations, protect users' right to know, choice, and privacy; maintain fair	commitment to abide by the rules of interconnection and interoperability. **Training System:** N/A **Social Reputation:** Demonstrates an open and cooperative attitude to the public by signing the Convention; the implementing agency may give internal notices, cancel membership, and notify the public for violations of the Convention, forming a reputational constraint mechanism through industry self-regulation.

No.	Document Name	Regulatory	Normative	Cultural-Cognitive
			competition, and shall not hinder or disrupt the normal operation of other platforms.	

Through a systematic review and analysis of 12 standard documents, these 12 flexible norms exhibit a clear evolutionary trajectory and complementary characteristics across the three dimensions of regulatory, normative, and cultural-cognitive systems.

From a regulatory perspective, all documents specify clear implementing entities and establish corresponding internal enforcement mechanisms. The national baseline standard the *GB/T 35273—2020 Information Security Technology - Personal Information Security Specification* (Sample 2) lays the foundational responsibility framework for personal information controllers, requiring legal representatives to assume overall responsibility and mandating the appointment of dedicated protection officers for large-scale processors. Industry and local standards, such as the *DB62/T 5083-2025 Tourism Big Data Security and Privacy Protection Standard* (Sample 3) and the *T/CCTAS 11-2020 Self-discipline Specifications for App-based Ride-hailing Company Safety and Security Operation* (Sample 7) further refine responsible entities to specific industry roles like tourism administration bodies and ride-hailing platform companies. They also require the establishment of security management systems, risk assessment mechanisms, and emergency response plans covering the entire data life-cycle. Corporation-level documents, such as the *F's Privacy Policy* (Sample 9) and the *X's Personal Information Protection Policy for Driver/Guide End* (Sample 11), translate regulatory requirements into concrete management measures. These include passing cybersecurity level protection assessments, obtaining ISO27001 certification, and implementing minimum necessary authorization and strict behavior monitoring for employees. Particularly noteworthy is the *Self-Regulatory Covenant for Promoting Interconnectivity and Interoperability of Internet Platforms* (Sample 12). As a form of industry self-discipline, it utilizes the Internet Society of China as its implementing body to construct a collaborative governance mechanism among platforms. Violations of the convention can result in internal notifications or even public disclosure, forming a unique model of industry self-regulation.

In terms of normativity, the documents demonstrate progressive sophistication in conceptual definitions, institutional design, and liability clauses. The national standard the *GB/T 35273-2020 Information Security Technology - Personal Information Security Specification* (Sample 2) provides the most comprehensive terminology system, defining in detail over 30 core concepts such as personal information, sensitive information, and de-identification, thereby laying the

conceptual foundation for other documents. Building upon this, industry standards (Sample 5, 6, 7) develop more sector-specific terminology, such as "trip sharing" and "complaint freezing" in the ride-hailing sector, and "untraceable whereabouts" and "zero-knowledge proof" in public transportation. Regarding institutional design, general standards like the *Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)* (Sample 8) systematically outline six major compliance areas, including service provision, algorithm recommendation, and service charging. Conversely, specialized documents like the *F's Rules on the Protection of Minors' Personal Information* (Sample 10) design separate consent mechanisms, access control permissions, and emergency response plans specifically for the minor demographic. Liability clauses also become increasingly detailed, evolving from the allocation of responsibility during entrusted processing, sharing, and transferring in national standards, to specific obligations in corporate policies requiring platforms to obtain consent before a driver shares guest information. This reflects the continuous decentralization and refinement of responsibility allocation.

On the cultural-cognitive dimension, public commitment has become a common requirement across all documents. Transparency has continuously increased, from the mandatory formulation of privacy policies in national standards to corporation policies prompting users to read policies via pop-ups upon the first launch of an app. The establishment and improvement of training systems represent a key finding of this analysis: National standard the *GB/T 35273-2020 Information Security Technology - Personal Information Security Specification* (Sample 2) explicitly requires regular specialized training and assessment for personnel in personal information processing roles; the *DB14/T 3539-2025 Guide to Privacy Protection in Tourist Hotel Guest Rooms* (Sample 4) necessitates training on specific behavioral norms for cleaning and maintenance staff; the *T/CSAS 0016-2025 Requirements on Personal Information Protection* (Sample 5) dedicates a section to stipulating that new employees must complete training and have assessment records retained within one month of on boarding; the *Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)* (Sample 8) further mandates the establishment of normalized compliance training mechanisms, integrating them into new employee orientation, management promotion, and annual training. Corporate policies, such as those from F corporation and X corporation, also mention regularly conducting security and privacy protection training sessions. (Sample 10, 11) Although only three flexible norms provide specific stipulations regarding social reputation, they still exhibit diversity: the widespread adoption of the national standard itself constitutes a form of social certification (Sample 2); industry guidelines require the establishment of external oversight mechanisms, for example, the *Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)* (Sample 8) calls for external supervision to enhance user trust, internalize compliance as corporate culture, and enhance market competitiveness. Meanwhile, the *Self-Regulatory Covenant for Promoting Interconnectivity and Interoperability of Internet Platforms* (Sample 12) forms an open and transparent reputation

constraint mechanism by publishing the list of joining and withdrawing entities to the public.

Analysis of the Internal Mechanisms of Flexible Norms

The research findings indicate that in the commercialization of tourism big data, although flexible governance norms for sensitive personal information lack the coercive force characteristic of traditional rigid rules, they can still effectively constrain participants through a series of sophisticated mechanism designs. Through a systematic analysis of 12 representative flexible norms formulated by different entities, we find that the regulatory pillar reveals the configuration of subjects regarding "who enforces," the normative pillar clarifies the rule framework concerning "what is enforced," and the cultural-cognitive pillar points to the value identification of "how to internalize." This set of norms constitutes a distinctive implementation safeguard system, namely the role-driven mechanism, the content-driven mechanism, and the enforcement-driven mechanism. (See Table 4)

Table 4. *Mechanisms to Achieve Effectiveness*

Mechanisms In/Ex	Internal Mechanisms	External Mechanisms
Role-Driven Mechanisms	Initiators and Implementers	Public Actors
Content-Driven Mechanisms	Internal Benefit-Cost Alignment Rule Design, etc.	Standardization & Certification
Enforcement-Driven Mechanisms	Public Commitments and Target Guarantee Measures	Pressure Transmission Measures

Specifically, the role-driven mechanism primarily activates the enforcement subject elements within the regulatory pillar by defining the functional configuration of initiators, enforcers, and supervisors, thereby addressing the issue of "organizational carriers" for flexible norms. The content-driven mechanism deeply integrates the detailed institutional design and responsibility clauses of the normative pillar, making compliance with flexible norms a "rational choice" for participants through specific implementation rules. The enforcement-driven mechanism comprehensively utilizes the cultural-cognitive pillar's public commitments and training systems, supplemented by pressure transmission channels, to propel flexible norms from "paper requirements" to "actual behavior." It is through the mutual reinforcement and progressive layering of these three mechanisms that flexible norms, despite the absence of coercive force, can still achieve practical effectiveness through organizational structure embedding,

incentive compatibility design, and social reputation constraints. This provides an actionable practical pathway for the protection of sensitive personal information in the commercialization of tourism big data.

Role-Driven Mechanism: Clarifying the Functional Configuration of Governance Subjects

The role-driven mechanism corresponds to the **Implementing Entities** and part of the **Internal Systems** within the regulatory pillar. Its core lies in transforming flexible norms into an operable governance structure by defining the functions and responsibilities of different participants.

First is the functional configuration of initiators and enforcers. National Standard the *GB/T 35273* (Sample 2) requires large-scale processors to establish a dedicated personal information protection officer. Sample 5 further stipulates that the legal representative bears overall responsibility, while the *Compliance Management Guidelines for User Rights Protection in Mobile Internet Application Services (2025)* (Sample 8) specifies the three-level responsibilities of the board of directors, compliance management officers, and business departments. This internal role division ensures that flexible norms have clear "owners" and "promoters" within the organization. For example, the "dedicated personal information protection department" and "personal information protection officer" established in the F's privacy policy (Sample 10), as well as the "specialized responsible team" mentioned in the X's guide (Sample 11) , provide organizational support for the implementation of flexible norms.

Second is the external constraint imposed by supervisory committees. The Self-Regulatory Covenant (Sample 12) designates the Internet Society of China as the convention enforcement body responsible for supervision and dispute mediation. The *GB/T 35273* (Samples 2) and the *T/CSAS 0016-2025* (Sample 5) introduce third-party certification and compliance audit mechanisms. These external supervisory bodies conduct independent assessments and public disclosures of participants' compliance performance through methods such as issuing reports, organizing evaluations, and accepting complaints, thereby forming an effective check on internal enforcers.

Content-Driven Mechanism: Integrating Rule Design and External Endorsement

The content-driven mechanism integrates the **Concept Definitions**, **System Design** and **Responsibility Clauses** from the normative pillar, as well as the **Public Commitments** from the cultural-cognitive pillar. Its core lies in making compliance with flexible norms a rational choice for participants through well-structured rule design.

On one hand, it involves the design of internal interest-cost trade-off rules. The *T/CSAS 0016-2025* (Sample 5) introduce international standard certifications and advanced technologies, enabling compliant entities to gain technological leadership and market competitive advantages. The *T/CCTAS 11-2020* (Sample 7) incorporates security performance into assessments and links it to rewards and penalties. The *DB14/T 3539-2025* (Sample 4) establishes an employee privacy protection evaluation mechanism. X's guideline (Sample 11) requires background checks and

confidentiality agreement constraints for employees who may access sensitive information. These designs internalize compliance costs, make violation costs explicit, and guide participants to proactively choose compliance based on interest trade-offs.

On the other hand, it involves external endorsement through standardization and certification. The *GB/T 35273-2020* (Sample 2), as a national standard, serves as the basis for national-level "personal information protection certification" and certification for cross-border personal information transfers. Sample 7 requires third-party network and information security assessments and the implementation of security operation compliance evaluations. The *T/CSAS 0016-2025* (Sample 5) sets mandatory compliance audit cycles (2/3/4 years) based on processing scale. These external certification mechanisms provide objective and verifiable proof of compliance with flexible norms, reducing information asymmetry among transaction parties and enhancing stakeholder trust.

Execution-Driven Mechanism: Ensuring the Implementation of Governance Requirements

The execution-driven mechanism corresponds to the **Public Commitments, Training Systems** and **Social Reputation** in the cultural-cognitive pillar, as well as the **Internal System** in the regulatory pillar. Its core lies in translating flexible norms from written requirements into actual practices through the transmission of internal and external pressure.

First, public commitments and target assurance mechanisms establish a reputation-based constraint mechanism. The *GB/T 35273-2020* (Sample 2) mandates the formulation and public release of personal information protection policies. The *T/CSAS 0016-2025* (Sample 5) requires apps to display privacy policies via pop-up notifications when first launched. Corporation policies (Samples 10 and 11) explicitly display contact information for the personal information protection officer in prominent locations. Such public commitments place an organization's compliance performance under public scrutiny, where violations may lead to reputational damage and user attrition. The Self-Regulatory Covenant (Sample 12) goes further by requiring the enforcement body to periodically publish lists of entities joining or withdrawing from the convention, thereby reinforcing reputational constraints within industry self-regulation.

Second,, training systems enable the internalization and perpetuation of norms. The *GB/T 35273-2020* (Sample 2) requires at least one specialized training session and assessment annually. The *T/CSAS 0016-2025* (Sample 5) stipulates that new employees complete training within one month of hire and retain assessment records. The Mobile Internet Application Guidelines (Sample 8) requires the establishment of training mechanisms integrated into promotion assessments. Corporation guidelines (Samples 10 and 11) explicitly mention regular security and privacy protection training programs. This systematic training transforms flexible norms from external constraints into employees' internal awareness and behavioral habits, ensuring the intergenerational transmission and sustained implementation of governance requirements.

Finally pressure transmission channels transform external regulatory pressure

into internal governance impetus. The *GB/T 35273-2020* (Sample 2) requires the establishment of complaint management mechanisms with responses within 15 days. The Mobile Internet Application Guidelines (Sample 8) mandates convenient complaint reporting channels and customer service hotlines with clearly defined response timelines. Corporation policies (Samples 9 and 10) provide multiple reporting channels. These channels facilitate the exercise of oversight by external individuals, aggregating dispersed individual concerns into sustained organizational pressure. The *DB14/T 3539-2025* (Samples 4) and the *T/CCTAS 11-2020* (Sample 7) extend this pressure transmission to the supply chain by requiring privacy protection clauses in supplier contracts, regular audits, and termination of partnerships in cases of non-compliance, thereby extending the effectiveness of flexible norms along the industrial chain.

In summary, the role-driven mechanism addresses the organizational carrier issue of flexible norms by clarifying "who executes," the content-driven mechanism resolves the incentive compatibility issue of flexible norms by appropriately designing "what to execute," and the enforcement-driven mechanism tackles the practical transformation issue of flexible norms by transmitting pressure on "how to execute." These three mechanisms are mutually reinforcing and progressive, collectively forming the institutional foundation for the effective operation of flexible governance norms. This finding reveals that flexible norms can achieve effective governance outcomes even in the absence of coercive force through sophisticated mechanism design, providing a practical operational path for the protection of sensitive personal information in the commercial application of tourism big data.

Conclusion

This study focuses on the practical effectiveness of flexible norms in governing sensitive personal information within the commercialization of tourism big data. It aims to answer the question: In the absence of state coercive enforcement, how do flexible norms generate de facto binding force on participants? By introducing W. Richard Scott's three pillars of institutions, the research constructs an analytical framework that transcends legal centralism. Employing a comparative case analysis method, it systematically examines 12 representative flexible norms texts, including national/provincial guidelines, industry standards, corporate policies, and self-regulatory covenants.

The study finds that the effectiveness of flexible norms do not stem from a single constraint mechanism but results from the synergistic interaction of three core driving mechanisms: First, the role-driven mechanism, anchored in the regulative pillar, provides an organizational vehicle for implementation by clarifying executing entities and their accountability relationships. Second, the content-driven mechanism, mainly rooted in the normative pillar, translates abstract principles into actionable operational guidelines through detailed rule design—such as data classification and grading, scenario-based technical indicators, and verifiable compliance requirements—thereby shaping participants' logic of rational choice. Third, the

enforcement-driven mechanism integrates public commitments, training systems, and social reputation constraints from the cultural-cognitive pillar. Through supervision, complaint handling, emergency response, and performance evaluation, it promotes the internalization of regulations from "paper requirements" into daily organizational practices and shared industry beliefs. These three mechanisms are nested and progressive, enabling flexible norms, even without coercive backing, to achieve practical effectiveness beyond their "flexible" appearance through organizational structural embeddedness, alignment of interests and incentives, and linkage to social reputation.

Although this study reveals the internal logic of how flexible norms achieve effectiveness through multi-case comparisons, several limitations exist. First, the analysis is primarily based on a static interpretation of texts, lacking direct empirical observation of the dynamic implementation processes, the actual degree of participant compliance, and long-term effects. For instance, whether corporations truly implement training systems or whether user complaints receive effective responses requires empirical testing. Second, while the sample strives for diverse types, it predominantly consists of Chinese domestic regulations and does not exhaust all emerging governance forms. The generalizability of the conclusions needs verification in broader cultural and institutional contexts. Finally, the study focuses on the mechanism design of flexible norms themselves, with limited discussion on their interactive relationships with other governance tools like rigid norms and technical standards—a critical issue unavoidable in a complex governance ecosystem.

Future research can be deepened and expanded in the following directions: First, conduct in-depth field investigations or questionnaire surveys to track the adoption, implementation, and effects of flexible norms within specific organizations, thereby validating and refining the mechanism model proposed in this study. Second, reveal the extent and conditions under which each of the three mechanisms operates. Therefore further study requires moving from analyzing "the presence of mechanisms" to "the strength of mechanisms," identifying the dominant mechanisms and their efficacy boundaries in different contexts through quantitative measurement, multi-case comparisons, or experimental methods.

References

Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. *International Organization*, 54(3), 421-456.

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines (2nd ed.)*. University of Michigan Press.

Benhaida, S., Safaa, L., & Perkumienė, D. (2024). Influencers and tourism: Story of a recent and revolutionary phenomenon: What does bibliometric analysis reveal. In *ENTER e-Tourism Conference* (pp. 421-433). Springer Nature Switzerland.

Bietti, E. (2020). From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 210-219).

Boto-García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. *Journal of Hospitality and Tourism Management*, 55, 240-247.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Buhalis, D., Leung, D., & Lin, M. (2023). Metaverse as a disruptive technology revolutionising tourism management and marketing. *Tourism Management*, 97, 104724.

Collingridge, D. (1980). *The Social Control of Technology*. London: Frances Pinter.

Cheng, X. (2021). *Understanding and Application of the Personal Information Protection Law*. China Legal Publishing House.

DiMaggio, P. J., & Powell, W. W. (Eds.). (1991). The new institutionalism in organizational analysis. University of Chicago Press.

Floridi, L. (2019). Translating principles into practices of digital ethics: Five risks of being unethical. *Philosophy & Technology*, 32(2), 185-193.

Florido-Benítez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities*, 7(1), 475-495.

Gao, F. (2022). *Personal Information Protection Law: Principles and Practice*. Law Press China.

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Greenwood, R., Oliver, C., Sahlin, K., & Suddaby, R. (Eds.). (2008). *The SAGE handbook of organizational institutionalism*. SAGE.

Gutierrez, C. I., Marchant, G., & Tournas, L. (2020). Lessons for Artificial Intelligence from Historical Uses of Soft Law Governance. *Jurimetrics J*, 61, 133.

Herke, C., Tóth, D., & Perkumienė, D. (2025). The Role of Artificial Intelligence in Cybercrime in the Tourism Sector. In *Tourism and Heritage: Shaping Sustainable and Innovative Futures* (pp. 415-433). Springer Nature Switzerland.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389-399.

Kalesnykas, R. (2025). Challenges of Ensuring the Implementation of Consumers' Right to Information in the EU Tourism Services Market. In *Tourism and Heritage: Shaping Sustainable and Innovative Futures* (pp. 227-251). Springer Nature Switzerland.

Luo, H., & Song, G. (2009). *Soft Law is Also Law: Soft Law Governance in Public Governance*. Law Press China.

March, J. G., & Olsen, J. P. (1989). *Rediscovering institutions: The organizational basis of politics*. Free Press.

Marchant, G. E. (2011). Addressing the pacing problem. In *The growing gap between emerging technologies and legal-ethical oversight* (pp. 199-205). Springer.

Mohd Shith Putera, N. S. F., Saripan, H., Mohd Bajury, M. S., & Ya'cob, S. N. (2022). Artificial intelligence in the tourism industry: A privacy impasse. *Environment-Behaviour Proceedings Journal*, 7(SI7), 433-440.

Moses, L. B. (2007). Recurring dilemmas: The law's race to keep up with technological change. *University of Illinois Journal of Law, Technology & Policy*, 2007, 239-285.

O'Connor, P. (2020). Data privacy and the travel sector. In *Handbook of e-tourism* (pp. 1-14). Springer.

Patton, M. Q. (2015). *Qualitative research & evaluation methods (4th ed.).* SAGE.

Perkumienė, D. (2025). Legal Issues of Personal Data Protection in the Electronic Space Related to Tourists' Data. In *Tourism and Heritage: Shaping Sustainable and Innovative Futures* (pp. 435-448). Springer Nature Switzerland.

Safaa, L., Oruezabala, G., & Bidan, M. (2021). Le tourisme à l'ère des technologies numériques. *Téoros. Revue de recherche en tourisme*, 40(2).

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). Sage Publications.

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly*, 61(2), 294-308.

Shelton, D. (Ed.). (2000). *Commitment and compliance: The role of non-binding norms in the international legal system*. Oxford University Press.

Shen, K. (2023). Autonomy, State Coercion and Soft Law: Revisiting the Forms and Boundaries of Soft Law. *Jurist*, (4), 29-41.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571-610.

Tan, Y. (2014). Flexible Governance: The Logical Choice and Development Trend of Government Governance Reform in the 21st Century. *Theoretical Discussion*, (03), 150-153.

Wu, T., & Hu, J. (2021). Flexible Governance: The Informal Relational Operation and Its Realization Mechanism of Grassroots Power—Taking the Practice of Social Work in S City as an Example. *Journal of East China Normal University (Philosophy and Social Sciences Edition)*, 53(02), 137-145+179.

Yallop, A. C., Gică, O. A., Moisescu, O. I., Coroș, M. M., & Séraphin, H. (2023). The digital traveller: Implications for data ethics and data governance in tourism and hospitality. *Journal of Consumer Marketing*, 40(2), 155-170.

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*. SAGE.

Zeng, X., Liang, Z., & Zhang, H. (2024). Optimizing the Path of Soft Law Governance for Artificial Intelligence: From Soft Law Precedence to Synergy between Soft Law and Hard Law. *E-Government*, (1), 34-35.

Zhang, X. (2023). Generative AI's Algorithm Governance Challenges and Regulatory Governance. *Modern Law Science*, (3), 120.