ADAPTING TO COERCIVE FORCES: HOW FOREIGN COMPANIES RESPOND TO CHINA'S DATA PROTECTION REGULATIONS

Completed Research Paper

Mo Chen, Technical University of Munich, Garching, Germany, mo.chen@tum.de
Lukas Vester[1], Technical University of Munich, Garching, Germany, lukas.vester@tum.de
Vinicius Agreste[1], Technical University of Munich, Garching, Germany, vinicius.santos@tum.de
Jens Grossklags, Technical University of Munich, Garching, Germany, jens.grossklags@in.tum.de

Abstract

China's recent data protection regulations – the Cybersecurity Law, Data Security Law, and Personal Information Protection Law – establish a comprehensive framework for data governance that also encompasses foreign companies operating within or conducting business with China. This study empirically examines how foreign companies perceive and respond to these stringent regulations. Using coercive isomorphism as a theoretical framework and semi-structured interviews as a research methodology, this empirical work analyzes foreign companies' interpretations of these regulations and their compliance strategies, including data localization, dual IT infrastructures, and administrative restructuring. Our findings show that while these strategies help achieve regulatory compliance, they introduce operational complexity, complicating the balance between local compliance and global cohesion. This work contributes to institutional theory by demonstrating how coercive pressure shapes organizational structures and operational strategies in multinational companies.

Keywords: China's data protection regulation, foreign companies, coercive isomorphism, compliance strategies, cross-border data transfer

1. Introduction

The global regulatory landscape for data protection has evolved rapidly, with frameworks like the EU's General Data Protection Regulation (GDPR) setting stringent standards for data security, privacy, and cross-border data flows (Ferracane, 2021; Voigt & von dem Bussche, 2017). Responding to its own digital transformation and significant cybersecurity challenges, China has been working to establish a comprehensive data protection framework (CNCERT, 2016). Between 2017 and 2021, three pivotal laws – the Cybersecurity Law (CSL, 2017), the Data Security Law (DSL, 2021), and the Personal Information Protection Law (PIPL, 2021) – were enacted, filling a gap left by prior fragmented regulations and imposing strict requirements on data localization and data handling (Creemers, 2022; Verri, 2023). Together with other data-related regulations and guidelines (e.g., *Interim Measures for the Management of Generative Artificial Intelligence Services*, *Regulations on the Administration of Algorithm Recommendation of Internet Information Services*, and *Ethical Norms for New Generation Artificial Intelligenc*e), these laws form the foundation of China's modern data governance system. While China's data protection laws draw some inspiration from regulatory models in the U.S. and EU (Albrecht, 2022; Geller, 2020; Li & J. Chen, 2024; Pernot-Leplay, 2020), they also

[1] These two authors contributed equally to this work.

reflect distinct priorities shaped by China's unique economic, political, and social landscape (Creemers, 2022). A key distinction is the emphasis on national security and data sovereignty (Gao, 2023; W. Tan, 2024; Xu, 2015).

One critical aspect of China's data protection regulations is their extended reach that affects foreign companies operating in or dealing with data from China. These companies are compelled to strategically modify their practices to align with the demands of powerful regulatory institutions, in order to retain legitimacy and access to key resources (DiMaggio & Powell, 1983), such as the Chinese market. Multinational companies must navigate diverse regulatory frameworks across countries, often facing conflicting requirements and developing dual compliance strategies to align with each regulatory framework's distinct mandates (Ferracane, 2021). These adaptations may bring about various impacts on companies' operations and overall development (Meyer & Rowan, 1977; Scott, 2008), such as cross-border data transfers and security assessments. For instance, Tesla established a data center in China to store information generated by its vehicles locally, ensuring compliance with the DSL's data export restrictions and the CSL's localization requirements (Yang, 2023). In contrast, LinkedIn, owned by Microsoft, decided to exit the Chinese market in 2021 due to the increasing complexity of complying with China's regulatory environment, which includes the PIPL's stringent personal data processing and transfer regulations (Olcott & Liu, 2023). These examples illustrate how companies adopt different strategies (e.g., business repositioning, competitive alignment), reorganize their operations for stability, and invest in technological solutions (e.g., infrastructures, information security) to ensure compliance. However, while such high-profile cases highlight the reach of the CSL, PIPL, and DSL, there remains a significant gap in empirical research regarding how foreign companies interpret these laws and adapt their operations. Our work explores these perspectives in depth.

This study is the first to examine how foreign companies (using German firms as a case) adapt to China's new data protection regulations. Using coercive isomorphism as a theoretical framework and semi-structured interviews as a research methodology, we address the following three research questions: (1) How do foreign companies interpret and perceive China's data protection laws? (2) How do they respond to the compliance requirements, particularly from the strategic, organizational, and technological perspectives? (3) What are the implications of these compliance strategies for their global operations and competitiveness? With our work, we explore the implications of regulatory pressure on multinational companies, particularly focusing on the intersection of international data governance and business strategies. As such, this study contributes to the fields of information systems, data protection and information security by exploring how regulatory pressure shapes corporate decision-making, compliance strategies, and technological infrastructures, while also demonstrating how companies adapt and strategically manage conflicting legal frameworks to maintain operational stability and competitive advantage.

2. An Overview of the Three Data Protection Laws in China

The CSL, DSL, and PIPL each emphasize data protection, national security, and cross-border data transfers, yet they focus on different aspects of China's data governance. Rooted in *China's National Security Law*, the CSL prioritizes cyberspace sovereignty and national security within the digital realm, serving as a broad framework for cybersecurity rather than detailing specific provisions (Qi, Shao & Zheng, 2018). It sets objectives such as the development of a hierarchical cybersecurity system, protection of critical information infrastructure, and requirements for security assessments of cross-border data transfers and network products or services. However, its generality leaves it relatively vague, placing the responsibility for detailed rule-making and enforcement to government departments. This approach is consistent with China's broader legislative approach (Creemers, 2022; Keller, 1994), yet it has also been criticized for lacking "systemic thinking" and "comprehensive institutional designs" (Hong, 2017, p.67).

The PIPL, while similar to the CSL in certain areas, focuses more on personal data protection, offering more specific provisions on personal data processing (Calzada, 2022). For instance, while the CSL

applies to "network operators", the PIPL includes all "personal information protection handlers", covering both governmental entities and companies. It includes specific provisions for how government departments should collect and handle personal information, balancing the goals of protecting individual privacy and supporting the operational demands of government, police, and security services, including surveillance activities (Calzada, 2022; Creemers, 2022). The PIPL also extends its extraterritorial reach to foreign entities handling personal data of Chinese residents, introducing specific compliance obligations or "tripwire provisions". For instance, foreign entities must undergo a government-led security assessment, obtain certification from a state-approved organization, or sign agreements with overseas recipients detailing data obligations when transferring data outside China.

The DSL, unlike the PIPL, covers both personal and non-personal data, introducing a data classification and hierarchical protection approach based on the potential impact on national security and economic development. It emphasizes data sovereignty by enforcing strict export controls that require "core national data", which pertains to national security, public interest, and economic growth, to undergo rigorous security assessments by the State Cyberspace Administration before any cross-border transfer (J. Chen & Sun, 2021). This structure underscores the law's dual aim of ensuring national security while fostering economic and social progress (Creemers, 2022). Additionally, the DSL requires local authorities to implement risk assessment, emergency response, and data security review mechanisms to ensure compliance and safeguard critical data.

In conclusion, the three laws collectively create a comprehensive and robust framework for data protection. The CSL lays the groundwork for cybersecurity, the PIPL strengthens personal data protection, and the DSL extends data governance with strategic classification and export controls. Together, these laws aim to address critical national security objectives, drive economic growth, and ensure individual privacy from a Chinese perspective.

3. Coercive Isomorphism

Institutional theory posits that organizations are shaped by broader social, cultural, and regulatory forces that drive them to align with established norms, rules, and expectations to gain legitimacy and stability within their institutional environments (DiMaggio & Powell, 1983; Meyer & Rowan, 1977; Powell & DiMaggio, 2012). As a result, these forces usually result in isomorphic tendencies, leading to increased similarities among organizations within a specific field (Greenwood & Hinings, 1996). Coercive isomorphism, one of the key mechanisms of institutional isomorphism, refers to organizational conformity driven by external pressure, including regulatory mandates and government directives, often motivated by the need for compliance and the avoidance of sanctions (Edwards, Mason & Washington, 2009; Scott, 2005). Such pressure can be both formal (e.g., laws and regulations) and informal (e.g., societal expectations and industry standards), often driving organizations to adopt specific practices, technologies, and strategic responses (DiMaggio & Powell, 1983).

This study draws on coercive isomorphism to analyze how China's new data protection laws shape the strategies and operations of foreign companies. Compliance with regulatory frameworks enables companies to mitigate legal risks, protect their reputation, and maintain stable operations in compliance- critical environments (Tolbert & Zucker, 1999). This alignment is essential for gaining access to regulated markets and maintaining competitive advantage (DiMaggio & Powell, 1983). Coercive isomorphism facilitates a homogenizing effect, where access to resources and market stability is contingent on adherence to external regulations (Beckert, 2010; Mizruchi & Fein, 1999). Formal compliance reflects deliberate efforts to align with institutional expectations shaped by legal frameworks and competitive pressure (Lewin & Kim, 2004). However, it is important to note that such conformity does not always equate to increased organizational efficiency and may sometimes lead to operational challenges (Kraatz & Zajac, 1996; Meyer & Rowan, 1977).

The concept of coercive isomorphism is frequently applied in corporate governance research to assess how regulatory environments influence organizational behavior (Jamali & Neville, 2011; Kostova &

Roth, 2002). In the field of information systems and information security, coercive pressure has been shown to drive significant shifts in IT governance and cybersecurity practices. For example, studies revealed how external pressure by the GDPR drove organizations to align their practices with new legal requirements to gain legitimacy and avoid penalties (Hsu, Lee & Straub, 2012; Lopes, Guarda & Oliveira, 2019). This study specifically focuses on the challenges faced by foreign companies navigating China's distinct data protection regulations. Operating in multiple jurisdictions, companies must reconcile differing regulatory demands, which makes them particularly sensitive to the complexity of local laws (Eden & Miller, 2004; Kostova, Roth & Dacin, 2008). Balancing compliance with both domestic and international standards complicates strategic planning and necessitates adaptive approaches. This theoretical approach provides a suitable lens for exploring how external legal pressure shapes organizational practices, especially within environments characterized by significant regulatory divergence (Kostova & Zaheer, 1999).

Coercive isomorphism highlights the way foreign companies modify their internal operations in response to mandatory compliance requirements. This alignment with legal mandates shapes business practices and operational strategies, helping to mitigate the risks of penalties and secure market legitimacy (Tolbert & Zucker, 1999). Through this lens, we illustrate how regulatory pressure influences organizational behavior and strategy.

4. Methodology

Focus on Germany: We use Germany as an illustrative case due to its close economic relationship with China. As of recent years, China has been Germany's top trading partner (Statistisches Bundesamt, 2024), while Germany has maintained a vital role in China's European market (Deutsche Vertretungen in China, 2024). Additionally, German foreign direct investment (FDI) in China has witnessed substantial and consistent growth, with a notable 34.7% increase during the first four months of 2024 (The State Council, 2024). Despite growing public debate on the risks and benefits of investments in China (Huld, 2024), the continued growth emphasizes the need to navigate regulatory challenges effectively (Deutsche Bundesbank, 2024).

Data Sampling: Institutional theory, in particular, the concept of coercive isomorphism, guided our data collection by offering a framework for the external regulatory pressure companies face when adapting to legal requirements. The theory shaped our participant selection and the design of semi-structured interview questions, focusing on how German companies align their strategies with Chinese regulatory demands to mitigate risks and ensure operational stability. To identify target companies for our study, we utilized the German Chambers of Commerce Abroad (Außenhandelskammer, AHK) Greater China's portal. Previous research documented a global decline in survey response rates, highlighting the challenge this trend poses for data collection in many fields (Brick & Williams, 2013; Stoop et al., 2010). This issue is further intensified when reaching out to company managers on sensitive topics, such as regulatory compliance in China. In our study, over 600 outreach emails were sent to German-based firms engaged with the Chinese market, yielding only 25 positive responses. As a result, we conducted 20 semi-structured interviews and collected five additional responses through questionnaires from March to June 2024. The sample covers a range of industries, including consulting, healthcare, IT, law, engineering, and public trade (see Table 1). The majority of participants had substantial expertise in Chinese data protection regulations, with only five not directly working with them. The high average level of expertise improved the depth and relevance of the insights gathered, aligning with the study's objectives. Previous research on qualitative methods suggests that a typical sample size for interview-based studies ranges from 20 to 30 or 20 to 40 participants (M. Chen, Bogner, et al., 2021, 2023; Creswell, 2013; Hagaman & Wutich, 2017). In a review by Marshall et al. (2013), it was found that 35% of information systems (IS) studies utilizing grounded theory were conducted with fewer than 20 interviews. Our research could be positioned within the fields of both IS studies and organizational and workplace studies. Therefore, our sample size aligns closely with many other studies. However, follow-up research could expand the sample

size and include companies from other countries to validate our findings and to further explore the topic space.

Structure of Interviews: Given the exploratory nature of our research on a topic that has yet to be thoroughly empirically analyzed, we opted to use semi-structured interviews. The interviews, lasting approximately 45 minutes on average, were designed collaboratively by the four authors and conducted online by two authors via Microsoft Teams or Zoom. With participant consent, interviews were recorded, and data anonymized, with respondents being assigned unique identifiers for data privacy. Our institution does not require ethics approval for interview-based studies, but we followed expected practices for ethical research when conducting the study and analyzing the data; in particular, assuring and maintaining confidentiality of the participants.

The interviews were structured to explore the organizational strategies companies employ to comply with Chinese data protection regulations, considering both formal and informal forms of pressure. The theoretical framework of coercive isomorphism helped us determine the types of questions that would yield insights into how regulatory pressure shapes organizational behavior and strategy. Specifically, we began the interviews with broad questions about the company's general operations in China and familiarity with Chinese data protection regulations, which were helpful to frame the context. Then, we focused on how the regulations have impacted business operations across various levels, exploring both the perceived advantages and disadvantages introduced by these regulatory changes.

Category	**Count**	**Definition**
Company Size	Large: 15 Medium: 4 Small: 4 N.A.: 2	Large (≥ 250 employees) Medium (50 – 249) Small (< 50)
Company Operating Status	Advanced: 21 Intermediate: 2 Introductory: 1 N.A.: 1	Advanced: operating flawlessly and at full speed Intermediate: well established with some minor issues Introductory: adapting, with some issues Precursive: initiating and taking the first steps to enter the market
Familiarity with the Regulation	High: 12 Medium: 7 Low: 4 N.A.: 2	High: knows the ins and outs of the regulations Medium: possess a general understanding of the regulations Low: unfamiliar with these specific regulations
Industries	Engineering/Manufacturing: 10, Consulting: 4, Law firm: 3, Education: 1, IT: 1, Public Trade: 1, Real Estate: 1, Insurance: 1, Healthcare: 1, N.A.: 2	

Table 1. Important table.

Data Analysis: Our findings are based on a thorough analysis of the interview transcripts, with both oral and written responses carefully reviewed. We employed directed content analysis (Hsieh & Shannon, 2005). Specifically, two researchers independently coded the responses to identify key themes, ensuring a systematic and thorough analysis of the data. To achieve inter-coder reliability, the two researchers compared, evaluated, and discussed their coding decisions at each step of the process. Finally, a third researcher then reviewed the initial coding results and engaged in discussions with the primary coders as needed. This collaborative review process enhanced the consistency and reliability of the analysis. Through these discussions and iterative refinements, we successfully reached

consensus. The coding results are analyzed in detail in the next section. The data supporting the findings of this study are available from the corresponding author upon reasonable request.

5. Findings

In the following, we present the five most significant and thought-provoking themes: participants' interpretation of China's data protection regulations, perceived compliance advantages, perceived compliance disadvantages, compliance actions, and compliance challenges.

5.1. Participants' interpretation of China's data protection regulations

Participants generally interpret China's data protection regulations through different key perspectives. At the highest level, these regulations are viewed as vital components of China's national strategy and security policy, supporting economic competition and national defense by maintaining control over data (CMP01, CMP06, CMP12, CMP17), and acting as a critical resource in global competition (CMP06, CMP11). A notable example is Didi Chuxing's delisting from the New York Stock Exchange, primarily driven by new Chinese data protection regulations, particularly the DSL, which mandated companies handling data of more than one million users to obtain approval from Chinese authorities before listing abroad (CMP06). Some participants also view them as aiding Chinese products in meeting international standards (CMP06). Regarding foreign companies, while one participant (CMP08) expressed concerns that the regulations could restrict their growth, others (CMP11, CMP16, CMP17) disagreed, downplaying the punitive nature of the regulations.

Participants highlighted the dual nature of China's policy implementation approach. First, China often allows companies to innovate freely before stepping in with regulations, unlike Germany or the EU, where regulations are often created early in an innovation cycle. As one participant (CMP06) explained, in China, "they always let people develop and experiment and then only at a later point, jump in and take control". While this approach fosters innovation, it can create confusion and uncertainty, especially when the regulatory environment changes abruptly (CMP06). Second, participants noted that China's approach tends to swing between extremes, with policies either being implemented or enforced at "full throttle or full brake" (CMP10), complicating compliance.

Participants shared differing perspectives on the enforcement and communication of data protection regulations, revealing significant variation in how compliance is assessed. Some reported frequent audits and strict enforcement (CMP01, CMP04, CMP10, CMP11, CMP15). For example, one participant (CMP01) noted that "the persons in charge of enforcement will, on a day-to-day basis or based on preference, determine how to enforce the laws". Another (CMP10) described regular inspections, stating that "local authorities come often (for) company audits. In the area where we are located, (we were) checked by the environmental health and safety authorities over 200 times in one year". In contrast, several participants reported minimal pressure from authorities (CMP02, CMP03, CMP06, CMP12, CMP13, CMP14), with comments such as, "No, not that I know of (compliance enforcement)" (CMP14), "we didn't get any (checks)" (CMP12), and "they are now going about, slowly but steadily, putting the regulatory framework into place" (CMP06). These differences may be influenced by regional variations, company size, and the industry of the company. For example, companies handling large data volumes or operating in sensitive sectors (such as finance, telecommunications, and critical infrastructure) may face more stringent requirements, especially regarding cross-border data transfers and the treatment of sensitive information. Notably, one participant (CMP05) learned about the regulations through a German commercial association rather than the Chinese government, indicating potential gaps in direct governmental communication with foreign companies.

5.2. Perceived advantages of China's data protection regulations

Participants' statements on perceived advantages of complying with China's data protection regulations concentrate on benefits to companies, while also addressing advantages for individuals and the state.

Perceived advantages to (foreign) companies: Compliance offers German companies a competitive edge in China by reinforcing their reputation for high standards (CMP14, CMP18). It also fosters awareness and responsiveness, as seen in the increasing demand for data protection officers (CMP03, CMP10). Legal alignment reduces risks of liabilities and penalties (CMP16), while standardized data security measures help prevent breaches. As CMP12 stated, "if you achieve the compliance with local laws, you have less risks [of data leakage, which can affect your business]". Additionally, compliance with data protection regulations reduces the risk of unauthorized access, leakage, or mishandling of sensitive personal data. By ensuring that only essential information is collected, stored, and processed, companies may have to forfeit a substantial amount of data; however, they also mitigate the risks associated with managing large volumes of personal information. As one participant noted, "it is also a chance to clean (the data) up" (CMP16). Consequently, companies can concentrate on essential and relevant data, streamlining internal processes, improving data quality and engagement, and ultimately enhancing the overall value of the data they retain (CMP10).

Perceived advantages to individuals: Participants identified personal information protection as a key advantage of companies' compliance with China's data protection regulations. Concerns about personal data misuse, such as unsolicited emails, spam, or random calls, were linked to unauthorized access or data sales. Accordingly, they expect the regulations to effectively sharpen corporate control over personal data and ensure transparency in cross-border data transfers. As one participant (CMP04) stated, the regulations would "protect (citizens' data) from unlawful export, transport, transfer, and make it very clear what rules have to be followed when intending on doing so." This perceived benefit underscores the regulatory framework's role in reinforcing individual data security and safeguarding privacy rights.

Perceived advantages to the government: Compliance with data regulations also serves national interests. Participants noted that these regulations grant the government greater control over data, enhancing national security (CMP08, CMP09). As data is considered the "fifth factor of production" in China, increased central oversight enables the state to harness data for economic and strategic purposes (CMP12), which further supports more effective data management. Additionally, compliance may strengthen national cybersecurity, fortifying the country's overall security infrastructure. Lastly, the regulations empower direct government intervention in corporate data practices. As CMP01 stated, "The Chinese state now can audit companies, their internal IT structures, also the data processing (systems)".

5.3. Perceived disadvantages of China's data protection regulations

Interview results revealed three main perceived disadvantages of compliance: increased costs, operational difficulties, and regulatory challenges. Increased costs were the most cited, mentioned 24 times. Compliance entails significant expenses, including IT infrastructure upgrades, administrative adjustments (CMP01, CMP09, CMP10, CMP12, CMP13), legal fees (e.g., external administrative audits) (CMP01), and consulting costs. As CMP10 noted, "we had to hire a lawyer" for legal consultation and regulatory interpretation (CMP04). Training costs to educate employees on compliance protocols (CMP10, CMP15) and opportunity costs, as top management dedicates substantial time and resources to compliance (CMP07, CMP09, CMP18), were also noted. CMP10 estimated 100-200 hours of top management's time, while CMP01 stated, "the overall cost you need for the internal budget can go into the millions".

The second key disadvantage pertains to operational difficulties stemming from compliance with new regulations. Companies must restructure operations and departments, which can complicate workflows and reduce efficiency (CMP03, CMP07, CMP16). A specific example was provided by participant

CMP11: "We do research in about 14 different industries, and when the DSL came out, we had to ensure that we established 14 different data classifications, basically."

Further, there has been significant discussion about the disadvantages related to cross-border data transfers. The new regulations often shift tasks from international to local employees to avoid international data transfers (CMP15), and require efforts to "separate your whole IT infrastructure" (CMP10). Consequently, these responsive measures not only create additional workload but also "prevent global networks" (CMP15) and reduce organizational synergies, resulting in missed opportunities and vulnerability to compliance risks (CMP10).

Lastly, regulatory compliance imposes significant legal complexity for organizations, with each new regulation adding additional burdens for legal departments (CMP05). In particular, the vagueness of some regulations complicates interpretation (CMP04), raising the risk of non-compliance as well as legal or financial penalties. Concerns were also raised about government access to company data, especially through audits. CMP18 expressed worries about intellectual property (IP) protection and the potential for fraud, noting that data processing includes not only personal information but also sensitive business data and trade secrets.

5.4. Compliance action

Interviewees' reported taking or planning actions in response to China's data protection regulations across three areas: strategic planning, administrative processes, and technological adaptations.

Companies' strategy planning: The interviewed companies have undertaken strategic adjustments in response to China's evolving data protection regulations. A notable trend is the increasing independence of Chinese branches from their headquarters, particularly in the human resources sector, to avoid classification under certain regulatory categories (CMP18). As CMP01 explained, "We cut off certain data transfers from our local HR system into the global HR platform". Similarly, CMP17 also mentioned their company's alignment with a global movement to establish comprehensive data protection management systems for local compliance.

Companies' administrative processes: German companies have implemented four major changes in their administrative processes. First, they have adapted workflows and protocols to meet new compliance requirements, similar to the adjustments made for the GDPR (CMP14, CMP18). Second, risk assessment and auditing have become critical. As CMP14 explained, "You check and double-check your contracts, you check your servers, you check your way how to handle data inside your company and maybe with external partners". Auditing was viewed as essential for ensuring effective risk mitigation (CMP17). Third, companies have launched training programs to enhance legal teams' understanding of relevant laws and regulations (CMP01, CMP10, CMP14, CMP15, CMP16). Finally, some companies have hired specialized lawyers to either support or manage data protection (CMP10, CMP18). However, a few companies reported minimal changes (CMP02, CMP10), with CMP05 stating, "To be honest, to our daily business, there is no effect generally because our business scoreboard is not so huge".

Companies' technological adaptations: Technological changes have focused on data localization and organization. Companies reported contrasting approaches to data localization: some centralized IT operations within China, either fully operating there or establishing local data infrastructure, as exemplified by Apple's initiative (CMP03, CMP10), while others relocated data centers outside China, retaining only essential data in China (CMP01, CMP15). The choice of data center locations often depends on industry-specific needs, with companies selecting regions such as Europe, Australia, the U.S., or Singapore based on factors like communication frequencies and low latency requirements (CMP01). For cross-border data transfers, CMP11 from a health service company described their approach, "... remove the names of the patients and use an ID number or something similar. We erase any personal information, retaining only the factual data that is necessary". Additionally, companies have prioritized data organization by identifying and categorizing data types, assessing relevance and sensitivity, especially in the Chinese context (CMP03).

5.5. Compliance challenges

In implementing compliance measures, companies have encountered challenges at three levels. *At the strategic level*, a major difficulty is the increasing complexity of the compliance landscape, as new regulations add legal and operational demands that must be integrated into global strategies (CMP18). This is compounded by the vagueness and rapid changes in local regulations, making it hard to determine which types of data can be stored and transferred (CMP11). The volatile regulatory environment requires constant monitoring and adaptation to manage changes. As CMP01 observed, "If you adjust to one regulation today, maybe next year it is going to change. So go for the strictest and most heavily sanctioned guidelines and, yeah, inspect your risk portfolio". Moreover, companies must navigate potentially conflicting frameworks when required to comply with multiple jurisdictions, such as reconciling Chinese and EU laws.

At the administrative level, a key challenge is the disruption of communication between local branches and headquarters, which hampers the efficiency of cross-border coordination (CMP14). Cultural differences also contribute, as some local colleagues in China may not prioritize regulations equally as their international counterparts, undermining compliance efforts (CMP10). Obtaining consent from data subjects is another major hurdle, with CMP10 noting, "Basically, the biggest administrative challenge in my opinion has been to receive the consent of the people whose data we process". Moreover, communication barriers between legal and technical teams create cross-functional challenges, hindering alignment. As CMP17 explained: "For technical background people they do not understand the legal (landscape), (and) for legal background people they do not understand tech knowledge. So sometimes I think one of the difficulties is to really understand each other."

At the technological level, a general challenge is adapting existing IT infrastructure to meet new regulatory requirements. Local Chinese IT teams, once focused on routine tasks, now manage complex cybersecurity roles previously handled in Europe, the U.S., and Australia (CMP01). Classifying, categorizing, and quantifying sensitive data poses significant challenges for many companies, particularly in relation to cross-border transfers (CMP11, CMP12). To address these, companies must engage in thorough data mapping to track storage locations. Moreover, compliance mandates to use Chinese-made hardware/software complicate implementation (CMP01), and restriction to a few authorized VPN providers add to the burden (CMP03). Furthermore, companies depend on third-party services' compliance, with SAP users reporting smoother transitions than those using Salesforce (CMP13). Lastly, separating IT infrastructure between China and other regions is particularly burdensome for industries like automotive, where R&D and manufacturing must stay connected across borders (CMP10).

6. Analysis and Discussion

This section analyzes and discusses the findings through the lens of coercive isomorphism, exploring how German companies operating in China are reshaping their operations and technology in response to China's stringent data protection regulations, highlighting both the adaptive measures they take and the challenges they face.

6.1. Cost-benefit analysis of compliance

In the context of coercive isomorphism, the cost-benefit analysis of compliance is generally about the trade-off between financial implications of adhering to regulatory requirements and risks of non-compliance. In addition, potential benefits as well as concerns about social costs should be considered (Khanna, 2021). Our interviews reveal four key benefits arising from compliance with China's data protection regulations, which align with coercive isomorphism theory while reflecting China's unique regulatory landscape. First, compliance mitigates legal and financial risks (McNulty & Ferlie, 2004). Companies adapt to regulatory mandates under isomorphic pressure to avoid sanctions and protect reputations (DiMaggio & Powell, 1983). Furthermore, a high level of compliance can provide companies with a competitive advantage. German companies in China leverage robust compliance to

differentiate themselves from local peers, thereby fostering trust and enhancing their market position – supporting the idea that regulatory compliance can serve as a strategic asset (Porter, 2008). The second benefit of compliance concerns long-term viability. Participants emphasized the dual nature of China's regulatory landscape, which requires flexibility due to its evolving standards and uncertainties (see Section 5.1). In this dynamic environment, adaptability is essential to minimize costly, disruptive adjustments and to bolster long-term stability (Meyer & Rowan, 1977). Proactively aligning with regulations reduces the costs of future compliance and equips companies with the flexibility to manage ongoing regulatory shifts, enhancing their resilience to change. Third, compliance could drive operational optimization. In regulated fields like data protection, strict standards encourage companies to refine data processes, improving data quality, data security, and resource allocation. As discussed in Section 5.2, compliance helps streamline operations by eliminating data clutter, reducing storage costs and improving processing speeds. As a result, companies would find themselves better positioned to achieve more efficient operations, enhancing overall organizational effectiveness (Meyer & Rowan, 1977; Scott, 2008). The fourth benefit stems from the societal impact of compliance, as enhanced personal data protection fosters public trust and demonstrates corporate responsibility. Given the similarities between Chinese and the EU data protection regulations (Z. Tan & C. Zhang, 2021; P. A. Weber, N. Zhang & Wu, 2020), participants highlighted a distinctive advantage for Chinese companies: compliance facilitates alignment with international norms, boosting their global competitiveness.

On the other hand, interviewed companies identified three main costs associated with compliance. First, they reported various financial burdens, including IT infrastructure upgrades, administrative restructuring, legal consulting, training, and continuous auditing to meet regulatory standards (see Sections 5.3 and 5.4). These investments are essential for meeting compliance obligations and fostering an organizational culture prepared for ongoing and future regulatory demands. However, these costs can strain budgets and divert funds from other strategic initiatives (DiMaggio & Powell, 1983). As companies strategically reallocate resources for compliance, they also contribute to the standardization of practices across industries, aligning under common legal frameworks (Gunningham, Kagan & Thornton, 2003). Second, companies often face operational disruptions when complying with stringent regulations. Participants noted that adjustments like restructuring departments or transferring workloads to local branches, while necessary, can interrupt established workflows, reduce efficiency, and delay the integration of new systems, like data protection infrastructure, with impacts that extend across various functions (Ambrose & Ausloos, 2013; Kitchin & McArdle, 2016). Third, compliance mandates can limit flexibility and prevent synergies by imposing rigid processes that inhibit adaptive change. This can create operational silos, where regulatory adherence is suppressing collaboration, stifling innovation and best practice sharing, and ultimately impeding growth and efficiency (DiMaggio & Powell, 1983; Meyer & Rowan, 1977).

The cost-benefit analysis highlights companies' strategic and operational efforts to effectively manage compliance with data protection regulations. By implementing data management related measures, they seek to balance the expenses of regulatory adjustments against potential legal risks (see Section 5.4). This approach aims to strike a balance that sustains long-term stability while meeting regulatory demands.

6.2. Operational restructuring and its challenges

The necessity for operational adjustments in response to regulatory requirements is a hallmark of coercive isomorphism (Oliver, 1991). Our interviews with German companies reveal a spectrum of restructuring activities, both planned and underway, in response to China's stringent data protection regulations. These include refining workflows, implementing continuous risk assessment, and increasing staff training, particularly in compliance practices. Some companies are also hiring legal professionals to handle regulatory responsibilities, underscoring the administrative and operational shifts required to meet compliance standards (see Sections 5.4 and 5.5).

At a broader level, companies are increasingly adopting strategies of structural decoupling. That is, they are creating local structures that operate semi-autonomously to better comply with local regulatory demands and to shield their main operations from external (local) scrutiny (Meyer & Rowan, 1977). This extends beyond the traditional concept of policy-practice decoupling (where formal policies diverge from daily operations) (Meyer & Rowan, 1977) and instead involves legal and operational separation as a ceremonial response to institutional pressures. In our case, some German companies are loosening the connection between their headquarters and Chinese subsidiaries (see Section 5.4). This institutional separation within the Chinese market may gradually segment it from global markets. Such moves demonstrate not only how regulatory pressure reshapes market landscapes but also how it transforms global corporate structures (Scott, 2008).

While the shift towards greater autonomy provides a strategic response to compliance risks, it also brings a set of operational challenges. As detailed in Section 5.5, companies experience disruptions in cross-border coordination and internal communication challenges, amplified by cultural differences and cross-functional misalignment. These challenges illustrate how coercive pressure not only prompts structural changes but also strains existing organizational dynamics.

6.3. Legal complexity and ambiguity

Legal complexity arises from the multi-layered regulatory requirements across regional, national, and international frameworks, where compliance expectations may conflict and evolve continuously. Such jurisdictional variation exists across all sectors, including data-driven fields (Abbott & Snidal, 2000). In countries like China, where data protection policies are expanding, companies face a complex landscape of nuanced requirements. While these regulations are designed to standardize compliance, they often generate uncertainty instead. Ambiguous regulatory language creates interpretative flexibility (Abbott & Snidal, 2000; Edelman, 1992), further compounded by regional variations in enforcement. Specifically, local authorities adapt enforcement strategies to regional contexts, leading to divergent implementation behaviors (see Sections 1 and 5.1). As a result, this regulatory ambiguity complicates companies' efforts to establish consistent compliance protocols, making it difficult to anticipate and align with shifting enforcement priorities or evolving interpretations by local authorities (M. Chen, Engelmann & Grossklags, 2023; Lange & Washburn, 2012). Moreover, the dual nature of China's policy approach further amplifies this uncertainty: while China's approach fosters rapid innovation by allowing companies the freedom to explore new ideas without immediate constraints, it can also create challenges when sudden regulatory shifts force businesses to quickly transition from experimentation to strict compliance (Interesse, 2023), intensifying the coercive pressure of navigating diverse and evolving regulatory frameworks.

In addition, foreign companies must navigate conflicting requirements not only across different regions within China but also on a global scale, e.g., by accommodating the stringent data protection requirements in the GDPR and China's DSL and PIPL (Mattli & Woods, 2009; Michaels, 2007). These regulations, while aiming to protect data security and privacy, sometimes impose contradictory mandates or create operational difficulties that place companies in challenging positions (R. Weber, 2013). For example, in the context of cross-border data flows, the GDPR emphasizes strict protections for data transfers outside the EU, whereas Chinese laws require that certain types of data remain within national borders. Some companies have also reported challenges in aligning data governance frameworks that satisfy both the GDPR's stringent consent requirements and security-focused mandates of DSL and PIPL (see Section 5.5). Such practical complications force companies to carefully assess and balance compliance in a way that respects multiple sets of regulations, often requiring significant operational adjustments to avoid non-compliance and potential penalties.

The legal ambiguity and complexity of compliance across jurisdictions increase administrative costs and operational challenges, while adding layers to decision-making processes. Companies must navigate conflicting regulatory landscapes, balancing compliance with various legal frameworks while maintaining operational integrity.

6.4. Technological adaptation in response to coercive pressure

German companies operating in China are adapting their technology-related strategies to comply with local data regulations, though these changes may not fully align with their broader operational needs. The theoretical framework of coercive isomorphism helps explain how regulatory pressure drives companies to adopt technologies based on external demands rather than intrinsic operational efficiency considerations or strategy optimization (DiMaggio & Powell, 1983). Moreover, such compliance-specific adaptations can reshape a firm's technological landscape, often embedding regionally compliant practices that can lead to operational fragmentation (Meyer & Rowan, 1977).

Data localization is a primary adaptation strategy, yet companies approach it differently. As presented in Section 5.4, some companies address data localization mandates by establishing local data centers to secure regulatory compliance and market access. However, this isolates their Chinese operations from the global IT structure, creating silos that hinder seamless integration (Tolbert & Zucker, 1999). In contrast, other companies prioritize efficiency and data security by managing data operations outside China, reducing exposure to local compliance risks. This decision is often driven by concerns about government access to sensitive data (Johnson & Goetz, 2007), which is also highlighted in our interviews. As a result, these companies establish a separate IT infrastructure specifically designed to meet Chinese regulations to complement their global operations infrastructure, introducing additional complexity, administrative costs, and a need for constant updates to align with evolving standards (Chander & Lê, 2014).

For both approaches, companies have to manage dual IT infrastructures to balance compliance with core operational stability – one for global operations and another tailored to meet local regulations (DiMaggio & Powell, 1983; Scott, 2008). The two expressions of dual IT infrastructures differ primarily in the location of data storage and processing: some establish local data centers, while others limit their in-country presence to lean operational setups that minimize regulatory exposure (Baldwin, 2018). Regardless of the approach, dual IT infrastructures introduce additional layers of complexity in aligning systems and reinforce operational fragmentation, as companies must manage separate systems to navigate diverse regulatory frameworks while maintaining stability in their global operations (Oliver, 1991).

The divergence in strategy stems from each company's unique strategic priorities, resource allocations, and risk assessments when responding to regulatory pressure. While coercive isomorphism drives adaptation to external mandates, it does not necessarily lead to convergence in technological responses (DiMaggio & Powell, 1983).

7. Conclusion

At the global level, China's data protection regulations reflect its increasing influence in global data governance. Previous research about the GDPR has pointed to a broader trend where countries/organizations with strong regulatory frameworks, such as the EU, not only influence corporate behavior within their borders but may also set precedents that can shape global data protection standards and norms (Hadjiyianni, 2021). China's comprehensive data protection laws not only shape corporate behavior within its borders but also contribute to the international discourse on data governance (Krause et al., 2023). By introducing stringent regulatory frameworks and advocating for digital standards like ISO, China is positioned to set precedents that may encourage other countries to adopt similar standards or align their policies (Cantero Gamito, 2023; De La Bruyère, 2022).

Through in-depth interviews, our empirical research explores how German companies in China navigate the complex landscape of the new data protection regulations through varied technological and organizational adaptations. From a practical perspective, our findings reveal the high costs of compliance, ranging from IT infrastructure investments to ongoing legal and technical training. This underscores the importance for companies maintaining flexibility to adapt to regulatory changes, particularly in dynamic environments like China. Recognizing compliance requirements as an integral part of corporate culture and business strategy is crucial for long-term resilience. At the same time,

policymakers should provide clearer guidance on compliance expectations, especially in areas where regulatory language remains ambiguous. In China, interpretation and enforcement of regulations can substantially differ on a regional or even municipal level (M. Chen & Grossklags, 2025), necessitating more differentiated support for companies. Globally, harmonizing regulatory requirements across jurisdictions could help reduce the compliance burden for companies operating across multiple markets. While this study focuses on the German case, the findings have broader implications for multinational companies operating in China and other areas with stringent data protection regimes. Many of these companies face similar challenges when adapting to local compliance demands, particularly in the realms of data localization and privacy protection. As regulatory pressure intensifies across different regions, companies must remain adaptable in navigating evolving regulations and anticipate the widespread impact that strong domestic frameworks in major economies will have on global compliance strategies. At the same time, this shared challenge also underscores the increasing importance of region-specific adaptations and the growing operational fragmentation in response to coercive regulatory pressure. Consequently, the lessons from the German case can offer valuable and actionable guidance for companies navigating complex regulatory landscapes worldwide.

From a theoretical perspective, this study extends institutional theory by demonstrating how coercive regulatory pressure shapes corporate adaptation strategies in heterogeneous ways, possibly influenced by companies' global strategies and industry-specific demands. This pressure drives varied responses, such as selective data localization, IT infrastructure segmentation, region-specific security protocols, and organizational restructuring, as firms balance regulatory obligations with operational efficiency. Compliance-driven technological adaptations are increasingly central in structuring and (re)shaping global corporate IT governance, influencing cross-border data flows, security strategies, and information systems design. As stringent data protection laws proliferate worldwide, our findings offer valuable insights for multinational companies seeking to integrate compliance with operational resilience in an increasingly complex and regulated digital economy.

8. Acknowledgements

We would like to sincerely thank the editors and reviewers for their valuable feedback and constructive suggestions, which greatly improved the quality of this paper.

References

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

Albrecht, D. (2022). Chinese first personal information protection law in contrast to the European GDPR. *Computer Law Review International,* 23(1), 1–5.

Ambrose, M. L., & Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy,* 3, 1–23.

Baldwin, R. (2018). *The Great Convergence: Information Technology and the New Globalization*. Harvard University Press.

Beckert, J. (2010). Institutional isomorphism revisited: Convergence and divergence in institutional change. *Sociological Theory,* 28(2), 150–166.

Brick, J. M., & Williams, D. (2013). Explaining rising nonresponse rates in cross-sectional surveys. *The ANNALS of the American Academy of Political and Social Science*, 645(1), 36–59.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the personal information protection law (PIPL). *Smart Cities,* 5(3), 1129–1150.

Cantero Gamito, M. (2023). The influence of China in AI governance through standardisation. *Telecommunications Policy*, 47(10), 102673.

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal,* 64, 677–739.

Chen, J., & Sun, J. (2021). Understanding the Chinese data security law. *International Cybersecurity Law Review,* 2(2), 209–221.

Chen, M., Bogner, K., Becheva, J., & Grossklags, J. (2021). The transparency of the Chinese social credit system from the perspective of German organizations. In: *Proceedings of the 29th European Conference on Information Systems (ECIS)*.

Chen, M., Bogner, K., Becheva, J., & Grossklags, J. (2023). On the transparency of the credit reporting system in China. *Humanities and Social Sciences Communications,* 10(1), 1–10.

Chen, M., Engelmann, S., & Grossklags, J. (2023). Social credit system and privacy. In: *The Routledge Handbook of Privacy and Social Media*. Ed. by S. Trepte and P. Masur. Routledge, pp. 227–236.

Chen, M., & Grossklags, J. (2025). Algorithmic regulation at the city-level in China. *Data & Policy,* forthcoming.

CNCERT (2016). *2015 China Internet Cybersecurity Report.* (in Chinese).

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity,* 8(1), 1–12.

Creswell, J. W. (2013). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches*. 3rd Ed. Sage Publications.

De La Bruyère, E. (2022). Setting the standards: Locking in China's technological influence. In: *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order.* Ed. by E. De La Bruyère, D. Strub, and J. Marek. The National Bureau of Asian Research, pp. 49–72.

Deutsche Bundesbank (2024). Zahlungsbilanzstatistik: Aktualisierte Ausgabe. Accessed on March 26, 2025. URL: https://publikationen.bundesbank.de/publikationen-de/berichte-studien/monatsberichte/monatsbericht-maerz-2024-926690?article=die-deutsche-zahlungsbilanz-fuer-das-jahr-2023-926694.

Deutsche Vertretungen in China (2024). Deutsch-chinesische Wirtschaftsbeziehungen. Accessed on March 26, 2025. URL: https://china.diplo.de/cn-de/willkommen-in-china/wirtschaft/wirtschaft-bilateral-1218264.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review,* 48(2), 147–160.

Edelman, L. B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American Journal of Sociology,* 97(6), 1531–1576.

Eden, L., & Miller, S. R. (2004). Distance matters: Liability of foreignness, institutional distance and ownership strategy. In: *Theories of the Multinational Enterprise: Diversity, Complexity and Relevance,* Vol. 16. Emerald Group Publishing Limited, pp. 187–221.

Edwards, J. R., Mason, D. S., & Washington, M. (2009). Institutional pressures, government funding and provincial sport organisations. *International Journal of Sport Management and Marketing,* 6(2), 128–149.

Ferracane, M. F. (2021). The costs of data protectionism. In: *Big Data and Global Trade Law*. Ed. by M. Burri. Cambridge University Press, pp. 63–82.

Gao, R. Y. (2023). A battle of the Big Three?—Competing conceptualizations of personal data shaping transnational data flows. *Chinese Journal of International Law,* 22(4), 707–787.

Geller, A. (2020). How comprehensive is Chinese data protection law? A systematisation of Chinese data protection law from a European perspective. *GRUR International,* 69(12), 1191–1203.

Greenwood, R., & Hinings, C. R. (1996). Understanding radical organizational change: Bringing together the old and the new institutionalism. *Academy of Management Review,* 21(4), 1022–1054.

Gunningham, N., Kagan, R. A., & Thornton, D. (2003). *Shades of Green: Business, Regulation, and Environment*. Stanford University Press.

Hadjiyianni, I. (2021). The European Union as a global regulatory power. *Oxford Journal of Legal Studies,* 41(1), 243–264.

Hagaman, A. K., & Wutich, A. (2017). How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, and Johnson's (2006) landmark study. *Field Methods*, 29(1), 23–41.

Hong, Y. (2017). On the gain and loss of cybersecurity law of China on data protection. *Information Security and Communications Privacy,* 1, 66–73. (in Chinese)

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research,* 23(3 Part-2), 918–939.

Huld, A. (2024). China-Germany Bilateral Direct Investment: Trends and Outlook. *China Briefing*. Accessed on March 18, 2025. URL: https://www.china-briefing.com/news/germany-china-investment-trends-and-outlook.

Interesse, G. (2023). Is China's 'Tech Crackdown' Over? Our 2023 Regulatory Outlook for the Sector. *China Briefing*. Accessed on March 18, 2025. URL: https://www.china-briefing.com/news/is-chinas-tech-crackdown-over-our-2023-regulatory-outlook-for-the-sector/.

Jamali, D., & Neville, B. (2011). Convergence versus divergence of CSR in developing countries: An embedded multi-layered institutional lens. *Journal of Business Ethics,* 102, 599–621.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy,* 5 (3), 16–24.

Keller, P. (1994). Sources of order in Chinese law. *The American Journal of Comparative Law,* 42(4), 711–759.

Khanna, V. S. (2021). Compliance as costs and benefits. In: *The Cambridge Handbook of Compliance*. Ed. by B. van Rooij and D. D. Sokol. Cambridge University Press, pp. 13–26.

Kitchin, R., & McArdle, G. (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society,* 3(1), 2053951716631130.

Kostova, T., & Roth, K. (2002). Adoption of an organizational practice by subsidiaries of multinational corporations: Institutional and relational effects. *Academy of Management Journal,* 45(1), 215–233.

Kostova, T., Roth, K., & Dacin, M. T. (2008). Institutional theory in the study of multinational corporations: A critique and new directions. *Academy of Management Review,* 33(4), 994–1006.

Kostova, T., & Zaheer, S. (1999). Organizational legitimacy under conditions of complexity: The case of the multinational enterprise. *Academy of Management Review,* 24(1), 64–81.

Kraatz, M. S., & Zajac, E. J. (1996). Exploring the limits of the new institutionalism: The causes and consequences of illegitimate organizational change. *American Sociological Review*, 61(5), 812–836.

Krause, T., Chen, M., Wassermann, L., Fischer, D., & Grossklags, J. (2023). China's corporate credit reporting system: A comparison with the United States and Germany. *Regulation & Governance,* 17(3), 755–771.

Lange, D., & Washburn, N. T. (2012). Understanding attributions of corporate social irresponsibility. *Academy of Management Review,* 37(2), 300–326.

Lewin, A. Y., & Kim, J. (2004). The nation state and culture as influences on organizational change and innovation. In: *Handbook of Organizational Change and Development.* Ed. by M. S. Poole and A. H. Van de Ven. Oxford University Press, pp. 324–353.

Li, W., & Chen, J. (2024). From Brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. *Computer Law & Security Review,* 54, 105994.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). EU General Data Protection Regulation implementation: An institutional theory view. In: *New Knowledge in Information Systems and Technologies: Volume 1*. Ed. by Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo. Springer, pp. 383–393.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *Journal of Computer Information Systems,* 54(1), 11–22.

Mattli, W., & Woods, N. (2009). *The Politics of Global Regulation*. Princeton University Press.

McNulty, T., & Ferlie, E. (2004). *Reengineering Health Care: The Complexities of Organizational Transformation*. Oxford University Press.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology,* 83(2), 340–363.

Michaels, R. (2007). "The true lex mercatoria: Law beyond the state." *Indiana Journal of Global Legal Studies,* 14 (2), 447–468.

Mizruchi, M. S., & Fein, L. C. (1999). The social construction of organizational knowledge: A study of the uses of coercive, mimetic, and normative isomorphism. *Administrative Science Quarterly,* 44(4), 653–683.

Olcott, E., & Liu, Q. (2023). LinkedIn to close China jobs service and cites strong competition. *Financial Times*. Accessed on March 18, 2025. URL: https://www.ft.com/content/4b288448-134a-41f9-9b6a-e883f4edf500.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review,* 16(1), 145–179.

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the US and the EU?. *Penn State Journal of Law & International Affairs,* 8(1), 49–117.

Porter, M. E. (2008). *Competitive Advantage: Creating and Sustaining Superior Performance*. Simon and Schuster.

Powell, W. W., & DiMaggio, P. J. (2012). *The New Institutionalism in Organizational Analysis*. University of Chicago Press.

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. *Computer Law & Security Review,* 34(6), 1342–1354.

Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. In: *Great Minds in Management: The Process of Theory Development.* Ed. by K. G. Smith and M. A. Hitt. Oxford University Press, pp. 460–484.

Scott, W. R. (2008). *Institutions and Organizations: Ideas and Interests*. Sage Publications.

Statistisches Bundesamt (2024). Ranking of Germany's trading partners in foreign trade 2023. Accessed on March 26, 2025. URL: https://www.destatis.de/EN/Themes/Economy/Foreign-Trade/Tables/order-rank-germany-trading-partners.pdf?__blob=publicationFile.

Stoop, I. A., Billiet, J., Koch, A., & Fitzgerald, R. (2010). *Improving Survey Response: Lessons Learned from the European Social Survey.* John Wiley & Sons.

Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. *Information & Communications Technology Law,* 33(3), 368–383.

Tan, Z., & Zhang, C. (2021). China's PIPL and DSL: Is China following the EU's approach to data protection?. *Journal of Data Protection & Privacy,* 5(1), 7–25.

The State Council (2024). Number of new foreign-invested firms in China continues to grow: Ministry. Accessed on March 18, 2025. URL: https://english.www.gov.cn/archive/statistics/202405/25/content_WS66512209c6d0868f4e8e770a.html.

Tolbert, P. S., & Zucker, L. G.(1999). The institutionalization of institutional theory. In: *Studying Organization: Theory & Method.* Ed. by S. R. Clegg and C. Hardy. Sage Publications, pp. 169–184.

Verri, B. (2023). The Chinese frontiers of data protection: The Personal Information Protection Law (PIPL). In: *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China*. Ed. by M. Timoteo, B. Verri, and R. Nanni. Springer, pp. 181–197.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Springer.

Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research,* 20, 565–587.

Weber, R. (2013). Transborder data transfers: Concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law,* 3(2), 117–130.

Xu, J. (2015). Evolving legal frameworks for protecting the right to Internet privacy in China. In: *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Ed. by J. R. Lindsay, T. M. Cheung, and D. S. Reveron. Oxford University Press, pp. 242–259.

Yang, Z. (2023). Chinese Tesla data to be stored on mainland. *China Daily.* Accessed on March 18, 2025. URL: https://www.chinadaily.com.cn/a/202308/15/WS64dad748a31035260b81c2f7. html.