

Governança de dados na China: soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim"

Luca Belli, Doutor em Direito pela Université Paris-Panthéon-Assas, Professor e Coordenador do Centro de Tecnologia e Sociedade da FGV Direito Rio

Sofia Chang, Mestra em Direito pela Universidade de Pequim, Pesquisadora no Centro de Tecnologia e Sociedade da FGV Direito Rio

RESUMO

O presente artigo analisa a estrutura da governança de dados da República Popular da China, com ênfase em sua formulação estratégica, arranjo institucional e arcabouço regulatório. Busca-se compreender o modelo de governança e regulação com "características chinesas" voltado a garantir, de maneira integrada, a proteção de dados, a cibersegurança, e soberania digital, e a inovação tecnológica, por meio de uma abordagem que alavanca de maneira integrada estratégia, legislação e política industrial. A análise é realizada a partir de quatro eixos: os fundamentos históricos e culturais que moldam a visão estatal sobre dados; os mecanismos de experimentação normativa utilizados para validar políticas públicas antes de sua implementação regional ou nacional; os instrumentos institucionais e regulatórios que sustentam o modelo; e os impactos internacionais da estratégia, considerando o contexto da Rota da Seda Digital. Conclui-se que o modelo chinês representa uma abordagem sistêmica, centrada na busca pela eficiência, segurança nacional e o desenvolvimento tecnológico, em contraste com os paradigmas supostamente centrados na proteção individual típicos das democracias liberais.

Palavras-chave: governança de dados; China; estratégia digital; proteção de dados pessoais; regulação; cibersegurança, políticas públicas.

ABSTRACT

This article analyzes the structure of data governance in the People's Republic of China, focusing on its strategic formulation, institutional design, and regulatory framework. Based on the Chinese state's approach to integrating data protection, industrial policy, cybersecurity,

and technological innovation, the study seeks to understand the normative model developed with "Chinese characteristics." The analysis is structured along four axes: the historical and cultural foundations that shape the state's view on data; the regulatory experimentation mechanisms used to validate policies before national implementation; the institutional and legal instruments that support the model; and the international impacts of the strategy, considering the context of the Digital Silk Road. It concludes that the Chinese model represents a systemic approach centered on administrative performance, national security, and technological development, contrasting with liberal democracies' individual-centric paradigms.

Keywords: data governance; China; digital strategy; personal data protection; regulation; cybersecurity, public policies.

Sumário

Introdução	5
1. Introdução ao modelo chinês de governança de dados	6
2. Estrutura institucional e estratégias estatais na governança de dados	9
2.1. Internet Plus	11
2.2. Plano "Feito na China 2025" (<i>Made in China – MIC - 2025</i>)	12
2.3. Plano de Desenvolvimento da Inteligência Artificial e Princípios de Governança	13
2.4. A Decisão do 4º Plenário do 19º Comitê Central do PCC e as Diretrizes sobre a Construção de um Mercado Unificado de Fatores de Produção	14
3. O ordenamento regulatório sobre governança de dados na China	16
3.1. Lei de Cibersegurança da China	16
3.2. Tecnologia de Segurança da Informação – Especificação de Segurança de Informações Pessoais (GB/T 35273-2020)	18
3.3. Lei de Segurança de Dados	19
3.4. Lei de Proteção de Informações Pessoais (LPIP ou <i>PIPL</i>)	22
4. Rumo ao "Efeito Pequim"	24
Conclusão	29

Table of Contents

Introduction	5
1. Introduction to the Chinese Data Governance Model	6
2. Institutional Structure and State Strategies for Data Governance	9
2.1. Internet Plus	11
2.2 The "Made in China 2025" Plan (MIC - 2025)	12
2.3. The Artificial Intelligence Development Plan and the Governance Principles.....	13
2.4. Decision of the 4th Plenary Session of the 19th CPC Central Committee and Guidelines on Building a Unified Market for Production Factors.....	14
3. Regulatory Framework for Data Governance in China.....	16
3.1 China's Cybersecurity Law.....	16
3.2. Information Security Technology – Specification for Personal Information Security (GB/T 35273-2020).....	18
3.3. The Data Security Law	19
3.4. The Personal Information Protection Law (LPIPI or PIPL)	22
4. Towards the "Beijing Effect"	24
Conclusion.....	29

Introdução

A ascensão da China como potência econômica e tecnológica, e seu crescente papel de referência em soberania digital,¹ tem despertado crescente interesse acadêmico quanto ao seu modelo de governança de dados e desenvolvimento de políticas digitais. Em contraste com os paradigmas normativos ocidentais, baseados na centralidade de direitos fundamentais, na limitação do poder estatal e na adoção de uma lei de proteção de dados como principal ferramenta regulatória, o modelo chinês estrutura-se em torno da noção de desempenho governamental, soberania (digital), cibersegurança e integração entre desenvolvimento econômico e controle normativo, combinando regulação, com política industrial e padronização técnica.² Este *blend* regulatório baseia-se na consideração que dados são ativos estratégicos e altamente valiosos, cuja gestão deve servir ao interesse nacional e ao fortalecimento do papel coordenador do Estado.³

Nos últimos anos, a China construiu um arranjo institucional e regulatório e regulatório abrangente e robusto para regular a coleta, o tratamento e a circulação de dados, articulando normas jurídicas, padrões técnicos e políticas industriais. Essa estrutura é coordenada por instituições de alto nível, como a Comissão Central de Cibersegurança e Informatização e a Administração do Ciberespaço da China (“ACC”), além de contar com planos estratégicos que definem investimentos estratégicos e implementam objetivos estruturais de curto, médio e longo prazo, como o *Internet Plus*, o *Made in China 2025* e o Plano de Inteligência Artificial. O modelo é ainda caracterizado por forte experimentação normativa em nível local, mecanismo pelo qual

¹ A soberania digital pode ser definida como “a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais tais como dados, softwares, hardwares e redes eletrônicas.” BELLI, Luca *et al*, **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**, RIO DE JANEIRO, RJ: Lumen Juris, 2026; BELLI, Luca; PAULI, Breno; COUTO, Natália, **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro**, **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro**; BELLI, Luca *et al*, **Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano**, Rio de Janeiro, RJ: FGV Direito Rio, 2023; JIANG, Min; BELLI, Luca (Orgs.), **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**, Cambridge: Cambridge University Press, 2025. Para uma contextualização do conceito no âmbito chinês, veja-se ROGIER CREEMERS, [INTERVIEW] “The Chinese approach to digital sovereignty”: 4 questions to Rogier Creemers – Sciences Po Chair Digital, Governance and Sovereignty.

² WANG, Wayne Wei, Contextualizing Personal Information: Privacy’s Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China, **Computer Law & Security Review**, v. 55, p. 106030, 2024. Também: PERNOT-LEPLAY, Emmanuel, China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?, **Penn State Journal of Law & International Affairs**, 2020.

³ WANG, Wayne Wei, China’s digital transformation: Data-empowered state capitalism and social governmentality, **The African Journal of Information and Communication (AJIC)**, n. 31, 2023.

são testadas e ajustadas políticas públicas antes de sua aplicação em escala regional ou nacional.

Este artigo oferece uma breve apresentação de um estudo mais amplo conduzido pelos autores sobre governança e regulação de dados na China, examinando os principais elementos que compõem este sistema, dividindo-se em quatro partes: os fundamentos históricos e filosóficos para a centralidade do Estado na gestão da informação e de dados; os métodos de experimentação e regulação facilitadora que contribuem para a estratégia do país de governança de dados; o funcionamento das instituições reguladoras e sua articulação com a política industrial; e, por fim, a projeção internacional do modelo chinês e seus efeitos normativos extraterritoriais. Ao longo da análise, buscamos entender como a China combina iniciativas de políticas públicas, atos normativos e inovação tecnológica como instrumentos para a robusta governança de dados do país.

A quarta parte explora a forma como o país se posiciona no cenário global como exportador de normas, padrões e estratégias de governança de dados, especialmente por meio de iniciativas como a Rota da Seda Digital e a Iniciativa Global de Segurança de Dados, que se tornam pilares essenciais da estratégia de soberania digital chinesa. A postura chinesa determina o nascimento de um verdadeiro "Efeito Pequim"⁴ no âmbito do qual o modelo chinês se torna um paradigma de governança e regulação de dados com crescente influência internacional. A conclusão deste estudo destaca os desafios de compatibilização entre soberania digital e cooperação internacional, além de sugerir que o modelo chinês poderá influenciar a governança de dados em outros países, principalmente do Sul Global, promovendo formas alternativas de regulação que desafiam os padrões euro-americanos consolidados.

1. Introdução ao modelo chinês de governança de dados

A governança de dados na China é caracterizada por um arranjo institucional e normativo ancorado em elementos históricos e culturais, combinando uma tradição administrativa baseada em monitoramento contínuo, uma tradição política baseada em planejamento econômico quinquenal, com inovação tecnológica e normativa. A construção desse modelo revela uma articulação entre estratégia estatal, desenvolvimento econômico e controle informacional que distingue a abordagem chinesa das adotadas por países ocidentais.

⁴ ERIE, Matthew S; STREINZ, Thomas, The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance, *N.Y.U. J. Int'l L. & Pol.*, v. 1, n. 54, p. 61, 2022.

Ao abordar a visão chinesa sobre uso e governança de informação, cabe ressaltar que a coleta sistematizada de dados pelo aparato estatal não é um fenômeno recente na China. Pelo contrário, desde a dinastia Tang (618–907), práticas administrativas envolviam o registro de informações detalhadas sobre indivíduos e atividades econômicas, com o intuito de subsidiar decisões governamentais e promover eficiência na gestão pública.⁵ Essa lógica persistiu até o presente, moldando uma política de dados orientada pelo controle e desempenho estatal, bem como pela centralidade do planejamento e do monitoramento. Assim, o uso extensivo de dados é legitimado, no contexto chinês, por uma concepção confucionista que subordina a privacidade individual ao interesse coletivo⁶ e, mais recentemente, para uma visão neoliberal e até materialista dos dados como ativos que devem ser explorados economicamente.⁷

Neste contexto, cumpre destacar que o processo de integração da privacidade ao arcabouço constitucional chinês, um empreendimento complexo, resultou em um sistema heterogêneo e fragmentado. Apesar de a dignidade pessoal e a proteção da residência serem garantidas, o direito à privacidade em si não possui uma codificação constitucional escrita e explícita, sendo tratado de forma implícita ou "desconstitucionalizada" em sua essência. Essa ausência de formalidade constitucional clara resulta em inconsistência ou desigualdade na aplicação judicial, dependendo de interpretações e da legislação infraconstitucional (como as leis de cibersegurança e proteção de dados, que serão abordadas adiante)⁸. Essa estrutura legal, em que a proteção é heterogênea, reflete a dicotomia para harmonizar os interesses de proteção dos indivíduos com a eficiência econômica e a soberania de dados do Estado, temas que centrais para o modelo chinês.

Em face dessa estrutura legal que subordina a proteção individual ao interesse estatal, a visão desenvolvimentista do governo chinês atribuiu à informação o papel de ativo estratégico cuja exploração deve beneficiar o interesse coletivo do País. A governança de dados a nível estatal, neste contexto, é o instrumento para maximizar a performance do governo e da economia chinesa, integrar tecnologias emergentes no setor público e privado, resguardar a segurança nacional, garantir que os objetivos

⁵ JIANG, Min, A brief prehistory of China's social credit system, **Communication and the Public**, v. 5, n. 3–4, p. 93–98, 2020.

⁶ WHITMAN, Christina, Privacy in Confucian and Taoist Thought, in: D. MUNRO (Org.), **Individualism and Holism: Studies in Confucian and Taoist Values**, Ann Arbor: Univ. of Michigan: Center for Chinese Studies, 1985.

⁷ Neste sentido, ver WANG, Contextualizing Personal Information. Supra n (2).

⁸ *Ibid.*

traçados estejam sendo alcançados, e, conseqüentemente, legitimar⁹ o próprio Partido Comunista Chinês.¹⁰ Assim, difere-se de modelos centrados na proteção de dados como direitos fundamentais (como na União Europeia).¹¹

Para compreender como a China busca alcançar tais objetivos estatais, faz-se mister, primeiramente, entender como são definidos. Um dos pilares metodológicos da formulação de políticas públicas na China é o experimentalismo regulatório. A prática conhecida como “ponto à superfície” consiste em uma abordagem essencialmente científica à regulação, que almeja testar a eficiência de normas e políticas em municipalidade específicas antes de sua aplicação ser escalada em âmbito provincial ou nacional.¹² Esse processo permite que somente iniciativas comprovadamente eficazes sejam institucionalizadas, assegurando maior aderência entre norma e realidade. Tal modelo é visível, por exemplo, na evolução do sistema de crédito social¹³ e nas zonas-piloto de desenvolvimento da indústria de e-commerce¹⁴ ou de computação em nuvem¹⁵.

⁹ **“Performance Legitimacy” and China’s Political Adaptation Strategy**, CoLab, disponível em: <<https://colab.ws/articles/10.1007%2Fs11366-011-9140-8>>. acesso em: 7 maio 2025. Conforme explicado no artigo, “Legitimidade por desempenho” é a expressão utilizada para se referir à estratégia adotada pelo Partido Comunista Chinês (PCC) de sustentar sua legitimidade política não por meio de processos democráticos, mas por meio da entrega de resultados concretos à população. Isso inclui o alcance de metas como crescimento econômico, estabilidade social, fortalecimento do poder nacional e governança eficiente. A legitimidade do regime, nesse modelo, deriva da sua capacidade de governar de forma competente e responsiva, ainda que sem eleições multipartidárias ou mecanismos tradicionais de *accountability* democrática. Trata-se de uma lógica pragmática, na qual a eficácia administrativa substitui a legitimação por representação popular. Nesse contexto, monitorar indicadores relacionados a diversos assuntos, para analisar, planejar, implementar ações de políticas públicas e atingir metas se torna crucial para garantir a legitimidade do governo.

¹⁰ *Ibid.* Conforme explicado no artigo, “Legitimidade por desempenho” é a expressão utilizada para se referir à estratégia adotada pelo Partido Comunista Chinês (PCC) de sustentar sua legitimidade política não por meio de processos democráticos, mas por meio da entrega de resultados concretos à população. Isso inclui o alcance de metas como crescimento econômico, estabilidade social, fortalecimento do poder nacional e governança eficiente. A legitimidade do regime, nesse modelo, deriva da sua capacidade de governar de forma competente e responsiva, ainda que sem eleições multipartidárias ou mecanismos tradicionais de prestação de contas democrática. Trata-se de uma lógica pragmática, na qual a eficácia administrativa substitui a legitimação por representação popular. Nesse contexto, monitorar indicadores relacionados a diversos assuntos, para analisar, planejar, implementar ações de políticas públicas e atingir metas se torna crucial para garantir a legitimidade do governo.

¹¹ JIANG, A brief prehistory of China’s social credit system.

¹² HEILMANN, Sebastian, **Red Swan: How Unorthodox Policy-Making Facilitated China’s Rise**, [s.l.]: The Chinese University Press, 2018. Capítulo 2.

¹³ **Full Text of Jiang Zemin’s Report at the 16th Party Congress**, China Through a Lens, disponível em: <<http://www.china.org.cn/english/2002/Nov/49107.htm>>. Acesso em: 7 maio 2025, 5; JIANG, A brief prehistory of China’s social credit system.

¹⁴ 页之码, Hangzhou introduces new policies to vigorously support the development of cross-border e-commerce.

¹⁵ GAO, Bai; RU, Yi, Industrial Policy and Competitive Advantage: A Comparative Study of the Cloud Computing Industry in Hangzhou and Shenzhen, in: **Innovation and China’s Global Emergence**, [s.l.: s.n.], 2021.

Essa abordagem evidencia uma racionalidade técnico-política voltada à experimentação, avaliação de desempenho e correção de rumos. Essa estratégia incorpora aspectos pragmáticos, tecnológicos e econômicos, numa perspectiva de governança baseada em evidências¹⁶ e que demonstrou ser altamente receptiva à inovação, dominando desafios complexos de modernização econômica em larga escala, ao mesmo tempo em que evita potenciais fracasso normativos e colapsos sistêmicos.¹⁷

Finalmente, outro aspecto importante da estratégia de políticas públicas da China é a regulação facilitadora, por meio de política industrial no âmbito da qual o governo central define metas de longo prazo, como as definidas no plano *Made in China 2025*¹⁸ (que será apresentado na seção seguinte), e delega aos governos locais a liberdade de implementar ações alinhadas aos seus contextos. Essa descentralização operacional fomenta competição institucional e inovação regulatória. Neste contexto, portanto, não somente as empresas competem para oferecer produtos e serviços de melhor qualidade pelo menor preço, mas as próprias administrações locais competem para oferecer as maiores facilidades - tais como isenção ou redução de impostos, subsídios e empréstimos com taxas de juros reduzidas etc. - às empresas consideradas como estratégicas. Shenzhen, cidade da província de Guangdong, por exemplo, antecipou normas de proteção de dados pessoais antes da adoção nacional de uma legislação de proteção de informações pessoais (que será objeto de análise na terceira seção).¹⁹

2. Estrutura institucional e estratégias estatais na governança de dados

A governança de dados na China está ancorada em uma estrutura institucional complexa e interconectada, desenhada para assegurar coerência sistêmica e integração entre as diretrizes estratégicas do Partido Comunista Chinês (PCC) e a implementação das políticas públicas necessárias para alcançar os objetivos do Estado. Desde 2014, com o fortalecimento da política de informatização e a elevação da

¹⁶ Estratégia considerada como instrumento para atingir uma governança produtiva, confiável e inclusive. Veja mais em OOIJEN, Charlotte van; UBALDI, Barbara; WELBY, Benjamin, **A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance**, Paris: OECD, 2019.

¹⁷ HEILMANN, Sebastian, Policy Experimentation in China's Economic Rise, **Studies in Comparative International Development**, v. 43, n. 1, p. 1–26, 2008.

¹⁸ U.S. CHAMBER OF COMMERCE, **Made in China 2025: Global Ambitions Built on Local Protections**, [s.l.]: U.S. Chamber of Commerce, 2017.

¹⁹ HULD, Arendse, Shenzhen Data Regulations: Clear Limits Imposed on Businesses; ZHU, Huang, Shenzhen Issues First Comprehensive Data Rules. A adoção das normas de Shenzhen foi feita durante o período em que o segundo rascunho da Lei de Proteção de Informações Pessoais estava sendo discutido na China.

cibersegurança à condição de questão de soberania nacional, foram criadas instituições especializadas com competências amplas e complementares, que desempenham um papel fundamental para a governança de dados chinesa.

- 1) A Comissão Central de Cibersegurança e Informatização, presidida pelo próprio presidente Xi Jinping, exerce função central na formulação de políticas macroestratégicas e planos quinquenais relacionados à transformação digital.²⁰
- 2) A Administração do Ciberespaço da China, responsável pela implementação normativa, fiscalização e coordenação interministerial no que se refere à segurança da informação, proteção de dados pessoais, regulamentação da inteligência artificial e governança de conteúdo digital.²¹
- 3) O recém-criado Escritório Nacional de Dados (*National Data Bureau – NDB*), estabelecido em outubro 2023 sob a alçada da Comissão Nacional de Desenvolvimento e Reforma²² tem por missão integrar a política econômica digital ao planejamento estratégico nacional. Isso é feito por meio da coordenação da digitalização de serviços públicos, da expansão de infraestruturas de *big data* e da formulação de políticas para o uso econômico de ativos informacionais.²³
- 4) Por fim, cabe frisar que um elemento essencial da governança de dados chinesa é a rede de "Bolsas de Dados" ou *Data Exchanges*, criadas a partir de 2015 como plataformas comerciais estabelecidas por entidade públicas, que operam como mercados de dados, permitindo a compra, venda e circulação regulada de ativos informacionais.²⁴ Esses atores desempenham um papel extremamente relevante, tendo natureza empresarial lucrativa, forte supervisão estatal e atribuições que incluem padronização, verificação, precificação, intermediação e conformidade legal no intercâmbio de dados entre organizações públicas e privadas.²⁵

²⁰ CREEMERS, Rogier, China's Cyber Governance Institutions, **Leiden Asia Centre**, v. January 2021, 2021, p. 6.

²¹ *Ibid.*, p. 8.

²² CHEN, Qiheng, China's new National Data Bureau: what it is and what it is not.

²³ *Ibid.*

²⁴ ARCESATI, Alex He, Rebecca, **Data Marketplaces and Governance: Lessons from China**, Centre for International Governance Innovation, disponível em: <<https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>>. acesso em: 5 dez. 2025.

²⁵ LU, Julia, Data exchanges in China, explained · TechNode.

A criação das entidades citadas acima foi fundamental para estabelecer a estrutura institucional necessária para alcançar a máxima eficiência e eficácia na elaboração, implementação e coordenação daquela que podemos definir como a "Grande Estratégia de Dados da China". Sua atuação junto às leis e normas que regulam o tratamento, a exploração econômica, e a proteção de ativos informacionais no país são base fundamental para consolidar o formato da regulação de dados no país.

Antes de analisar cenário normativo da regulação dados na China, é essencial compreender quatro iniciativas estratégicas que consolidam política industrial e planejamento, lançadas pelo país com o objetivo de consolidar sua posição como potência global no setor de tecnologia da informação: Internet Plus, Made in China 2025, o Plano de Desenvolvimento de Inteligência Artificial (IA), e a Decisão do 4º Plenário do 19º Comitê Central do PCC, que define oficialmente dados como um fator de produção. Esses documentos revelam os pilares fundamentais da estratégia da regulação de dados, da construção da infraestrutura tecnológica e de desenvolvimento informacional da China. Além disso, ilustram como as políticas públicas são articuladas de maneira orgânica, para acelerar a transformação digital do país, reduzindo a dependência de tecnologia estrangeira e alcançando protagonismo em setores intensivos em dados, como o de computação em nuvem, o da Internet das Coisas (IoT) e o de IA.

2.1. Internet Plus

Lançada oficialmente em 2015 pelo então Primeiro-Ministro Li Keqiang, a iniciativa *Internet Plus* visava a promoção da digitalização dos setores tradicionais por meio da integração entre Internet móvel, computação em nuvem, Big Data e IoT com a manufatura moderna, o comércio eletrônico, serviços financeiros e governamentais. Seu objetivo ia além da conexão de tecnologias; englobando a criação de um ecossistema digital que interconectaria indivíduos, dispositivos e serviços para gerar e analisar dados em grande escala.²⁶

O plano quinquenal da iniciativa previu, entre outras metas: conectar 98% da população chinesa à banda larga; atingir velocidades de 100 MB/s nas grandes cidades; e reduzir a dependência de tecnologias estrangeiras, para favorecer a autonomia estratégica nacional. Esta iniciativa pioneira em termos de soberania digital baseava-se em quatro pilares, quais sejam, a integração transectorial, a reestruturação de

²⁶ Full Text: Report on the Work of the Government (2015), The State Council of the People's Republic of China, disponível em: <https://english.www.gov.cn/archive/publications/2015/03/05/content_281475066179954.htm>. Acesso em: 8 maio 2025.

sistemas, o incentivo à criação de plataformas abertas e compartilhadas e a conectividade ubíqua.

Por fim, a *Internet Plus* não se limitava à mera informatização dos setores e serviços tradicionais, mas também expressava a necessidade de desenvolver ferramentas regulatórias adequadas para acompanhá-los.²⁷ Assim, essa iniciativa passou a ser compreendida como um marco regulatório, sendo um precedente importante no processo de construção dos diversos instrumentos normativos que serão analisados na terceira seção deste artigo.

2.2 Plano "Feito na China 2025" (*Made in China – MIC - 2025*)

Complementando o *Internet Plus*, o plano *Made in China 2025* (MIC 2025) buscou transformar e integrar as indústrias de alta tecnologia da China. Se o *Internet Plus* focou na conectividade e na digitalização de serviços, o plano *Made in China 2025* (MIC 2025) representou a aplicação dessa lógica à esfera produtiva, operacionalizando a estratégia estatal conhecida como "integração da informatização e industrialização" (em chinês 两化融合, *lianghua ronghe*).²⁸

Elaborado pelo Ministério da Indústria e Tecnologia da Informação (MIIT) — órgão cuja própria estrutura fundiu a regulação industrial e a de informação —, com apoio de mais de 150 especialistas, o MIC 2025 tinha como meta reorganizar a produção tecnológica nacional. Seu objetivo era utilizar a infraestrutura de dados – possibilitada pelo plano anterior – para , promover a inovação doméstica e reduzir a dependência de tecnologia estrangeira.²⁹

O MIC 2025 exemplifica, novamente, a abordagem sistêmica chinesa e a constante preocupação com a construção de uma sólida soberania digital. Particularmente, o MIC 2025 visava simultaneamente o aprimoramento da política industrial, e a atualização de padrões técnicos e da regulação normativa. O plano destacou dez setores prioritários, como os de TI avançada, robótica, veículos elétricos, equipamentos aeroespaciais, medicina avançada e agricultura de precisão.³⁰ Neste plano, o Estado atuaria como agente indutor, coordenando investimentos, centros de inovação, propriedade intelectual e incentivos fiscais, com o objetivo de alinhar o desenvolvimento tecnológico ao interesse nacional.

²⁷ **Implementation of "Internet Plus Regulation" in Safety Production Precise Law Enforcement in the City's Industrial and Mining Fields**, Window of Yiwu - Free Trade, disponível em: <https://www.yw.gov.cn/art/2024/4/21/art_1229436709_59477522.html>. Acesso em: 8 maio 2025.

²⁸ CHANG, Amy, *Warring State: China's Cybersecurity Strategy*, **Center for a New American Security**, 2014.

²⁹ U.S. CHAMBER OF COMMERCE, **Made in China 2025: Global Ambitions Built on Local Protections**.

³⁰ *Ibid.*

O MIC 2025 buscou promover a digitalização da economia, especialmente em setores intensivos em dados como Big Data, IA, robótica e e-commerce, nos quais dez anos depois a China se tornou parte da liderança mundial. Destacou-se também pelo uso estratégico de investimentos com função regulatória, impulsionando inovações desejadas antes mesmo da imposição de proibições normativas. O sucesso em integrar a informatização e a indústria resultou na criação de bases massivas de dados operacionais e na demanda por maior automação. Esse novo contexto industrial e de dados tornou inevitável a necessidade de um plano estratégico de nível superior focado em processar essa informação: o desenvolvimento da Inteligência Artificial. Por fim, cumpre ressaltar que digitalização da República Popular da China, impulsionada pelo MIC 2025, ainda, foi fortalecida pelos esforços legislativos em áreas como segurança cibernética, proteção de dados pessoais e segurança de dados, que, conforme informado, serão analisados na terceira seção deste artigo.

2.3. Plano de Desenvolvimento da Inteligência Artificial e Princípios de Governança

Reconhecendo o potencial estratégico da Inteligência Artificial (IA), tanto para fins civis quanto militares, e aproveitando a rica base de dados e a infraestrutura industrial estabelecidas pelo Internet Plus e pelo MIC 2025, a China lançou em 2017 o Plano de Desenvolvimento da Nova Geração de Inteligência Artificial (AIDP).³¹ Esse plano estabeleceu metas ambiciosas até 2030 para tornar o país o centro global da inovação em IA. As metas definidas no plano foram: até 2020: equiparar-se aos países mais avançados; até 2025: liderar globalmente em alguns segmentos; até 2030: tornar-se líder mundial absoluto em IA.

Nesse contexto, o AIDP previu, até 2025, a criação de um sistema inicial de leis, regulamentos, padrões e mecanismos de avaliação de segurança para garantir o "desenvolvimento seguro, confiável e controlável da IA".³² A regulamentação da IA foi tratada no plano como um processo multissetorial, coordenado pelo Estado, com participação de especialistas acadêmicos, empresas e diferentes órgãos administrativos, com a finalidade de aumentar a qualidade dos processos de elaboração e implementação regulatória.

Nesta perspectiva, em 2019, o Ministério da Ciência e Tecnologia (MOST) publicou os Princípios de Governança para uma Nova Geração de IA, desenvolvidos

³¹ WEBSTER, Graham *et al*, Full Translation: China's "New Generation Artificial Intelligence Development Plan" (2017).

³² *Ibid.*

por um grupo de especialistas em um processo colaborativo.³³ Esses princípios incluem: harmonia, justiça, inclusão, respeito à privacidade, segurança, responsabilidade compartilhada, colaboração aberta e governança ágil.

Por fim, o plano também estabeleceu o exercício do financiamento estatal como papel regulador, por meio de Fundos-Guia Governamentais, responsáveis por direcionar investimentos públicos e privados para setores estratégicos.³⁴

2.4. A Decisão do 4º Plenário do 19º Comitê Central do PCC e as Diretrizes sobre a Construção de um Mercado Unificado de Fatores de Produção

A 4ª Sessão Plenária do 19º Comitê Central do PCC, concluída em outubro de 2019, resultou na adoção de uma decisão estratégica destinada a "seguir e aperfeiçoar o sistema do socialismo com características chinesas e avançar a modernização do sistema e da capacidade de governança da China".³⁵ Esse marco define o momento em que o regime chinês formalizou, num plano estrutural de governança, a incorporação dos dados como um novo "fator de produção", ao lado dos fatores tradicionais como terra, capital, trabalho e tecnologia. A adoção desse entendimento implica que os dados passaram a ser tratados como um insumo estratégico e econômico, merecendo atenção institucional para sua regulamentação, governança e utilização produtiva.³⁶

Com base nessa decisão, em 9 de abril de 2020, o Comitê Central do PCC publicou, conjuntamente com o Conselho de Estado, as Diretrizes sobre a Construção de um Mercado de Fatores de Produção orientado pelo mercado.³⁷ O documento afirma a intenção de promover "a alocação dos fatores de produção mediante mercado", e explicitamente menciona a aceleração do desenvolvimento de mercados para os fatores "tecnologia e dados". Dessa forma, as diretrizes criam um arcabouço normativo e político para tratar dados como ativo econômico, mobilizável e regulável, abrindo caminho para a institucionalização de mecanismos de transação de dados, de natureza pública-privada ou regulada pelo Estado.

³³ MOST (MINISTRY OF SCIENCE AND TECHNOLOGY), **Governance Principles for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence**, China Daily, disponível em: <<https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html>>. Acesso em: 8 maio 2025.

³⁴ LUONG, Ngor; ARNALD, Zachary; MURPHY, Ben, **Understanding Chinese Government Guidance Funds: An Analysis of Chinese-Language Sources**, [s.l.]: Center for Security and Emerging Technology, 2021.

³⁵ Decision of the Fourth Plenum of the 19th Central Committee of the Chinese Communist Party.

³⁶ RIHUI, Ouyang, Data as a Factor of Production Promoting the Deep Integration of the Digital Economy and the Real Economy: Theoretical Logic and Analysis Framework, **Frontiers of Economics in China**, v. 19, n. 2, p. 129–153, 2024.

³⁷ **China unveils guideline on improving market-based allocation of production factors**, disponível em: <https://english.www.gov.cn/policies/latestreleases/202004/10/content_WS5e8faa09c6d0c201c2cc0922.html?utm_source=chatgpt.com>. acesso em: 5 dez. 2025.

O impacto dessas decisões no surgimento e consolidação das supramencionadas "bolsas de dados", ou *data exchanges*, é profundo e multifacetado. Primeiro, ao reconhecer publicamente dados como fator de produção, o Estado legitima juridicamente a criação de estruturas especializadas para sua circulação, o que dá respaldo legal e incentivo político para que municípios e províncias chinesas lancem *data exchanges*. Segundo, as Diretrizes de 2020 fornecem a "moldura institucional" que orienta a organização do mercado de fatores, incluindo os dados, sinalizando que a mobilidade desses fatores deva se dar de maneira ordenada, sob regulação e com objetivos de desenvolvimento de alta qualidade. Isso estimula governos locais e autoridades a investir em plataformas reguladas, em padronização, certificação e governança de dados.³⁸

Assim, na prática, os *data exchanges* chineses funcionam como intermediários regulados: registram conjuntos de dados, certificam sua qualidade e conformidade, e permitem a negociação entre provedores e demandantes, sob supervisão estatal. A institucionalização conferida pela decisão de 2019 e pelas diretrizes de 2020 favorece a combinação entre objetivos políticos, jurídicos, econômicos e de soberania estatal, uma vez que o Estado mantém controle sobre os fluxos de dados, impondo padrões de segurança, anonimização, classificação e conformidade normativa. Portanto, essa experiência é uma característica extremamente relevante da governança de dados chinesa, mostrando como a conjugação de decisão política de alto nível e regulação institucional podem ser coordenadas para estabelecer bases legais, organizacionais e econômicas. Essas bases permitem que os dados sejam tratados como ativo produtivo, ativo esse a ser explorado para maximizar a soberania digital, integrando segurança, governança, proteção de dados e incentivo à inovação no país.

Considerando as iniciativas apresentadas neste capítulo, cabe destacar a visão sistêmica que caracteriza as diferentes fases da governança e regulação de dados chinesas: a consulta multissetorial liderada pelo governo, a experimentação regulatória das propostas de lei por meio do modelo "ponto à superfície", a regulação facilitadora por meio de política industrial, e o fortalecimento das regulações ligadas às tecnologias digitais, como as de cibersegurança e segurança de dados, com base na integração dos elementos normativos mais eficientes.

A articulação entre instituições centrais e governos locais, entre normas legais e padrões técnicos, e entre inovação e controle revela uma governança de dados pragmática, científica e sistêmica, porém orientada por objetivos ideológicos definidos pelo regime. Essa estrutura é projetada não apenas para disciplinar o uso interno de

³⁸ LU, Data exchanges in China, explained · TechNode; ARCESATI, **Data Marketplaces and Governance**.

dados, mas também para ampliar a influência externa da China no campo regulatório digital, o que será objeto de análise na quarta seção deste artigo.

3. O ordenamento regulatório sobre governança de dados na China

A consolidação institucional da estratégia chinesa de governança de dados exige a formulação de um arcabouço jurídico capaz de sustentar e operacionalizar os objetivos traçados pelo Estado de forma eficiente e performante. Enquanto estruturava sua política digital por meio de planos estratégicos e mecanismos de coordenação entre órgãos centrais e governos locais, a República Popular da China passou a intensificar, a partir de 2016, o desenvolvimento de um sistema legal voltado à regulação do ambiente informacional.

O fortalecimento desse ordenamento jurídico-regulatório buscou não apenas a proteção dos dados (inclusive os pessoais) e a promoção da segurança cibernética, mas, também, a consolidação da autonomia tecnológica, ambos conceitos à base da soberania digital, como princípios fundantes da atuação estatal no domínio tecnológico. A elaboração dessas normas, brevemente apresentadas a seguir, revela o esforço do legislador chinês em criar uma arquitetura regulatória coerente com os princípios e as diretrizes definidas nos instrumentos de planejamento estratégico apresentados anteriormente.

3.1 Lei de Cibersegurança da China

Aprovada em novembro de 2016, a Lei de Cibersegurança da China foi o primeiro marco legal nacional voltado à regulação da segurança da informação e do tratamento de dados. Com base no princípio da soberania, a norma busca proteger a segurança nacional e o interesse público, e integrar-se ao processo de digitalização econômica e social do país,³⁹ aplicando-se a todas as atividades (como construção, operação, manutenção e uso) das redes digitais no território chinês.

Nesse sentido, a proteção das infraestruturas de informações críticas é um dos eixos centrais da legislação, abrangendo setores estratégicos como energia, telecomunicações, transporte, finanças e serviços públicos.⁴⁰ A Lei impõe obrigações específicas aos operadores dessas infraestruturas, como a criação de departamentos especializados em segurança, realização de treinamentos técnicos, implementação de

³⁹ Artigo 1. CREEMERS, Rogier; WEBSTER, Graham; TRILOLO, Paul, **Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)**, Stanford University DigiChina, disponível em: <<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>>. Acesso em: 6 maio 2022.

⁴⁰ Artigo 31. *Ibid.*

planos de contingência e adoção de medidas de recuperação de desastres.⁴¹ Além disso, obriga tais operadores a armazenarem na China qualquer informação pessoal ou dado importante que coletem ou produzam. Caso seja estritamente necessário fornecer esses dados para fora do país por motivos de negócios, os operadores devem realizar uma avaliação de segurança seguindo as medidas conjuntas formuladas por órgãos estatais,⁴² nos termos estabelecidos pela lei.⁴³

Além disso, a Lei introduziu o famoso Sistema de Proteção Multinível (também conhecido pela sigla do termo em inglês, *MLPS – Multi-Level Protection System*), exige que os operadores de rede cumpram uma série de obrigações de segurança. Eles devem estabelecer sistemas internos de gestão e regras de operação, designando pessoas responsáveis pela segurança cibernética. Além disso, é necessário implementar medidas técnicas para prevenir ataques cibernéticos, vírus e invasões. O sistema também obriga o monitoramento e registro do status da rede e de incidentes de segurança, com os logs sendo armazenados por, no mínimo, seis meses. Por fim, os operadores de rede devem adotar medidas de proteção de dados como a classificação, o backup de informações importantes e a criptografia, além de qualquer outra obrigação prevista em lei.⁴⁴ Ainda, a lei exige que os operadores de rede garantam a confidencialidade dos dados dos usuários, implementando sistemas de proteção eficazes.⁴⁵

No plano institucional, a Lei atribui ao Estado, especialmente à Administração do Ciberespaço da China, a responsabilidade pela coordenação, monitoramento e atualização das políticas de cibersegurança, bem como pela criação de sistemas de alerta e notificação de incidentes.⁴⁶ A Lei de Cibersegurança prevê, ainda, a imposição de sanções severas em caso de descumprimento de suas obrigações, incluindo multas significativas tanto para as organizações quanto para indivíduos diretamente responsáveis por infrações.⁴⁷

⁴¹ Artigo 34. *Ibid.*

⁴² Artigo 37. *Ibid.*

⁴³ O artigo 53 define os departamentos responsáveis pelo estabelecimento dos mecanismos da avaliação de segurança.

⁴⁴ Artigo 21. *Ibid.*

⁴⁵ Artigo 40. *Ibid.*

⁴⁶ Artigos 8, 51 e 52, *Ibid.*

⁴⁷ As sanções e penalidades estão descritas no Capítulo VI da Lei (artigos 59 a 75). As multas e penalidades por descumprimento da lei de segurança cibernética variam consideravelmente, dependendo da gravidade da infração e do tipo de operador envolvido. Por exemplo, no caso de operadores de infraestrutura de informação crítica, as multas por não cumprimento dos deveres de proteção são significativamente mais altas, variando de RMB 100.000 a 1.000.000, com os gestores diretamente responsáveis podendo ser multados entre RMB 10.000 e 100.000. Outras penalidades incluem a suspensão temporária de operações, suspensão de negócios para correções, fechamento de sites e até o cancelamento de licenças de operação ou de negócios.

Por fim, destaca-se que em 2022⁴⁸ foi apresentada uma proposta de emenda à Lei com o intuito de harmonizar suas disposições com a Lei de Proteção de Informações Pessoais e a Lei de Segurança de Dados da China. Entretanto, a proposta de emenda legislativa não teve nenhum avanço até abril do ano de 2025, quando o governo chinês publicou um segundo rascunho de emenda.⁴⁹ Este novo texto introduz avanços relevantes, como a criação de um sistema de penalidades graduais (como, por exemplo, contando com multas menores para falhas em obrigações de segurança, e aumento em caso de recusa em endereçar as falhas ou de ameaça à segurança, atingindo o máximo (até 10 milhões de yuans) com a aplicação de sanções empresariais severas (suspensão de negócios, revogação de licenças) para incidentes de alta gravidade), o endurecimento dos requisitos de certificação para produtos e equipamentos de rede, e amplia a responsabilidade dos operadores de CII exigindo a verificação de conformidade de seus fornecedores.

3.2. Tecnologia de Segurança da Informação – Especificação de Segurança de Informações Pessoais (GB/T 35273-2020)

Denominada "*Information security technology – Personal information (PI) security specification* (GB/T 35273-2020),⁵⁰ a Especificação de segurança de informações pessoais representa um dos instrumentos mais relevantes da proteção de dados pessoais na China. Embora não tenha natureza jurídica vinculativa, trata-se de um padrão técnico nacional amplamente reconhecido por orientar a aplicação das normas legais em matéria de segurança e proteção de informações pessoais.

Elaborada pelo Comitê Técnico Nacional de Padronização em Segurança da Informação (também conhecido como TC260), sua primeira versão entrou em vigor em maio de 2018, sendo posteriormente revisada em 2020.⁵¹ A especificação surgiu como um mecanismo normativo essencial para suprir as lacunas regulatórias existentes antes

⁴⁸ **Office of the Central Cyberspace Affairs Commission – Cyberspace Administration of China.** Notificação para Solicitar Opiniões Públicas sobre a Decisão de Alterar a Lei de Segurança Cibernética da República Popular da China (Rascunho para Opiniões. Disponível em: <http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm>. Publicado em: 14 set. 2022. Acesso em: 6 maio 2025.

⁴⁹ **Office of the Central Cyberspace Affairs Commission – Cyberspace Administration of China.** Notificação para a solicitação de opiniões públicas sobre o Rascunho para uma Segunda Rodada de Comentários sobre a Emenda à Lei de Segurança Cibernética da República Popular da China. Disponível em: <https://www.cac.gov.cn/2025-03/28/c_1744779434867328.htm>. Publicado em: 28 março 2025. Acesso em: 06 maio 2025.

⁵⁰ Information security technology— Personal information (PI) security specification - GB/T 35273— 2020 (Replacing GB/T 35273-2017). Disponível em: <<https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>>. Acesso em: 06 maio 2025.

⁵¹ *Ibid.*

da entrada em vigor da Lei de Segurança de Dados (DSL) e da Lei de Proteção de Informações Pessoais (PIPL) do país,⁵² que serão apresentadas a seguir.

O texto da especificação define princípios e requisitos técnicos para as diversas etapas do tratamento de informações pessoais, como coleta, armazenamento, uso, compartilhamento, divulgação e exclusão.⁵³ Ela também prevê mecanismos para garantir os direitos dos titulares⁵⁴, estabelece exigências específicas para o tratamento de dados sensíveis,⁵⁵ além de dedicar um anexo inteiro a orientações sobre como identificá-los,⁵⁶ e inclui um modelo de aviso de privacidade, buscando padronizar como garantir transparência em relação ao tratamento de dados.⁵⁷ Em sua versão atual, a norma introduz exigências técnicas rigorosas, que, embora voluntárias, são frequentemente utilizadas por autoridades chinesas como critério de avaliação de conformidade com as normas de proteção e segurança da informação.

Sua importância decorre de uma característica central da abordagem regulatória chinesa: o uso de padrões técnicos suplementares às leis que fornecem instruções detalhadas e concretas sobre como alcançar as exigências legais. A Especificação exemplifica esse modelo ao oferecer instruções práticas para implementação dos princípios jurídicos abstratos de segurança e proteção de informações pessoais. Dessa forma, além de reforçar o cumprimento da lei, a norma assume um papel didático e orientador, fornecendo às organizações uma base técnica concreta para estruturar seus produtos, serviços e arquiteturas internas em conformidade com o ordenamento jurídico.

3.3. Lei de Segurança de Dados

Promulgada em 1º de setembro de 2021, a Lei de Segurança de Dados estabelece o marco regulatório da segurança de dados na China, com o objetivo de padronizar o tratamento de dados, assegurar a segurança da informação, promover o

⁵² CREEMERS, Rogier, China's emerging data protection framework, *Journal of Cybersecurity*, v. 8, n. 1, 2022.

⁵³ Information security technology— Personal information (PI) security specification - GB/T 35273— 2020 (Replacing GB/T 35273-2017). Para mais detalhes, ver o conteúdo das Seções 5 a 9 da Especificação.

⁵⁴ Seção 8 da Especificação. *Ibid.*

⁵⁵ Definidos no item 3.2 da Especificação "informações pessoais que, uma vez vazadas, fornecidas ilegalmente ou abusadas, podem colocar em risco a segurança pessoal e patrimonial, ou facilmente levar a danos à reputação pessoal, à saúde mental e física, ou a tratamento discriminatório, etc.", cujas medidas adicionais de segurança específicas para seu tratamento estão detalhadas no item 6.3 da Especificação. *Ibid*

⁵⁶ Anexo B. *Ibid.*

⁵⁷ Anexo D. *Ibid.*

uso e desenvolvimento de dados, proteger direitos legítimos de indivíduos e organizações, e salvaguardar a soberania e os interesses nacionais.⁵⁸

Esta Lei também designa a Administração do Ciberespaço da China como o órgão central de coordenação da segurança de dados. Porém, também delega competências também a autoridades setoriais e locais, segundo suas respectivas áreas de atuação.⁵⁹

A segurança dos dados é tratada de forma diferenciada, por meio de um sistema de categorização e classificação de dados. A proteção dos dados deve ser baseada em sua importância para o desenvolvimento econômico e social, bem como no potencial de dano à segurança nacional, aos interesses públicos ou aos direitos de indivíduos e organizações, caso esses dados sejam alterados, destruídos, vazados, obtidos ilegalmente ou usados indevidamente. Neste contexto, órgãos estatais são responsáveis por coordenar a elaboração de catálogo de "dados importantes" e por reforçar a proteção desses dados. Os dados considerados "essenciais" para o estado – aqueles que se referem à segurança nacional, às bases da economia, aos aspectos cruciais da vida das pessoas e a grandes interesses públicos – serão submetidos a um sistema de gestão mais rigoroso.⁶⁰

É importante destacar que a soberania de dados da China também é um pilar central da Lei de Segurança de Dados, manifestando-se em dois pontos principais: por meio de uma estratégia de contramedidas e pelo controle sobre a transferência de dados para o exterior, inclusive em cooperações com autoridades estrangeiras. Em relação ao primeiro ponto, a lei estabelece que, se um país ou região impuser proibições ou restrições discriminatórias à China em áreas como investimento, comércio ou tecnologias de dados, o governo chinês poderá retaliar, considerando as circunstâncias.⁶¹

Já em relação à transferência internacional de dados, a lei estabelece que a transferência de dados importantes para fora do país, quando coletados ou produzidos por operadores de infraestrutura de informação crítica, devem seguir as disposições da Lei de Cibersegurança. Para os demais processadores de dados, as medidas de gestão de segurança para transferência internacional de dados importantes serão

⁵⁸ Artigo 1 da Lei de Segurança de Dados da República Popular da China. Disponível em: <http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html>. Publicada em: 10 junho 2021. Acesso em: 06 maio 2025.

⁵⁹ Artigo 6.

⁶⁰ Artigo 21.

⁶¹ Artigo 26.

formuladas em conjunto pela Administração do Ciberespaço da China e pelos departamentos relevantes do Conselho de Estado.⁶²⁶³

Quanto ao compartilhamento de dados com órgãos judiciais ou policiais estrangeiros, a lei determina que apenas as autoridades chinesas competentes podem responder tais pedidos. Ademais, é expressamente proibido que qualquer organização ou indivíduo na China forneça dados armazenados no território chinês a entidades judiciais e policiais estrangeiras sem a aprovação prévia das autoridades competentes.⁶⁴

No que tange às obrigações dos órgãos estatais, busca-se um equilíbrio entre a segurança e a abertura dos dados governamentais. A segurança é tratada como uma prioridade. Os órgãos estatais têm a obrigação de proteger a confidencialidade de dados acessados, como informações pessoais, segredos comerciais e a privacidade dos indivíduos.⁶⁵ A lei exige que esses órgãos estabeleçam sistemas robustos de gestão de segurança de dados e cumpram suas responsabilidades de proteção.⁶⁶ Além disso, procedimentos rigorosos de aprovação e supervisão são exigidos quando um órgão estatal contrata terceiros para lidar com sistemas ou dados governamentais. O terceiro contratado é proibido de reter, usar, vaziar ou fornecer esses dados sem autorização.⁶⁷ Simultaneamente, a lei incentiva ativamente a abertura de dados. Ela promove o desenvolvimento do governo eletrônico e a utilização de dados para impulsionar o crescimento.⁶⁸ Os órgãos estatais são orientados a divulgar informações de forma oportuna e precisa, respeitando princípios de justiça, igualdade e conveniência para o cidadão, a menos que a divulgação seja proibida por lei.⁶⁹ Para facilitar esse processo, a legislação prevê a criação de um catálogo de dados governamentais abertos e uma plataforma de dados unificada, segura e controlável, que incentive a publicação e o uso desses dados.⁷⁰

⁶² Artigo 31.

⁶³ Cumpre destacar que a Administração do Ciberespaço da China já adotou medidas que detalham os requisitos para avaliações de segurança na transferência internacional de dados. Essas medidas, que entraram em vigor em 1º de setembro de 2022, estabelecem um mecanismo de avaliação de segurança para empresas que lidam com um grande volume de dados de usuários ou com informações categorizadas como "importantes" ou "sensíveis". Em março de 2024, novas regulamentações foram publicadas para flexibilizar esses requisitos, aumentando os limites de volume de dados pessoais e estipulando cenários de isenção da revisão de segurança para a transferência de dados. Veja mais em: HULD, Arendse, Cross-Border Data Transfer - New Measures for Security Review.

⁶⁴ Artigo 36.

⁶⁵ Artigo 38.

⁶⁶ Artigo 39.

⁶⁷ Artigo 40.

⁶⁸ Artigo 37.

⁶⁹ Artigo 41.

⁷⁰ Artigo 42.

A responsabilização pelo descumprimento da Lei de Segurança de Dados na China é escalonada e rigorosa. Inicialmente, as autoridades competentes podem emitir ordens de correção e advertências. No entanto, a recusa em corrigir as falhas ou a ocorrência de consequências graves, como vazamentos de dados em massa, leva à aplicação de multas substanciais, que podem chegar a milhões de yuans. As penalidades também se estendem aos indivíduos diretamente responsáveis, que enfrentam multas pessoais. Em casos mais severos, a lei permite a suspensão de negócios, a revogação de licenças e, em situações que envolvam ameaças à soberania ou segurança nacional, a responsabilidade pode evoluir para a esfera criminal. O governo também pode aplicar sanções administrativas a seus próprios funcionários que negligenciarem seus deveres.⁷¹

Por fim, no ano de 2024, o governo promulgou o Regulamento sobre a Gestão da Segurança de Dados de Rede,⁷² que, conjuntamente com padrões técnicos para classificação e catalogação de dados, sinalizam um movimento de sofisticação regulatória. Assim, é possível perceber que, com a Lei de Segurança de Dados, o modelo inicialmente mais programático e principiológico evoluiu para uma estrutura regulatória mais técnica, operacional e orientada à fiscalização concreta.

3.4. Lei de Proteção de Informações Pessoais (LPIP ou PIPL)

A Lei de Proteção de Informações Pessoais (LPIP mas conhecida como PIPL, no acrônimo inglês de "Personal Information Protection Law"), em vigor desde 1º de novembro de 2021, constitui o primeiro marco legislativo nacional abrangente sobre proteção de informações pessoais no país. Inspirada em normas estrangeiras como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), a Lei estabelece princípios, bases legais e garantias fundamentais para o tratamento de informações pessoais, aplicando-se inclusive a operações transnacionais que tenham como alvo indivíduos localizados na China.⁷³

A norma estabelece um regime abrangente de direitos aos titulares de dados, incluindo acesso, correção, exclusão, portabilidade, oposição a determinados tipos de tratamento de dados e controle sobre decisões automatizadas com impacto

⁷¹ Capítulo VI da Lei de Segurança de Dados.

⁷² 中华人民共和国国务院令, 网络数据安全条例_信息产业(含电信), 中国政府网, disponível em: <https://www.gov.cn/zhengce/content/202409/content_6977766.htm>. Acesso em: 12 maio 2025.

⁷³ Artigo 3. THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA, Personal Information Protection Law of the People's Republic of China. Disponível em: <http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm>. Acesso em: 06 maio 2025.

relevante⁷⁴. A definição de "informações pessoais sensíveis" é especialmente ampla, contemplando dados financeiros, biométricos, localização geográfica e dados de pessoas menores de 14 anos, e sujeita a requisitos rigorosos de tratamento⁷⁵. Nesse aspecto, a PIPL assemelha-se ao RGPD e à Lei Geral de Proteção de Dados brasileira (LGPD), e distingue-se pelo compromisso firmado pelo estado de estabelecer e aprimorar um sistema de proteção de dados, que busca prevenir e punir violações dos direitos sobre informações pessoais, além de promover a conscientização e a participação conjunta do governo, empresas e público na proteção de dados.⁷⁶

Diferentemente do modelo europeu, que adota as categorias conceituais de "controlador" e "operador",⁷⁷ a PIPL não faz essa distinção formal. Em seu lugar, utiliza o conceito de "gestor de informações pessoais" (ou "*personal data handler*"), cuja atuação pode ser delegada a terceiros mediante obrigações contratuais específicas,⁷⁸ evidenciando uma preocupação mais pragmática e centralizada na cadeia de comando do tratamento de dados.

Outra exigência relevante é a exigência de avaliações de segurança e requisitos de localização de dados em território chinês, especialmente para operadores de infraestruturas de informações críticas⁷⁹ (consoante aos requisitos estabelecidos pela Lei de Segurança Cibernética e a Lei de Segurança de Dados). Ainda, a transferência internacional de dados pessoais é permitida apenas se o gestor de informações cumprir requisitos específicos. Para realizar essa transferência, o gestor deve atender a uma das seguintes condições: passar por uma avaliação de segurança organizada pelo departamento nacional de ciberespaço; obter uma certificação de proteção de dados de uma instituição especializada; ou firmar um contrato-padrão com o destinatário no exterior, que defina as obrigações de ambas as partes.

A lei também prevê a possibilidade de seguir as disposições de tratados ou acordos internacionais dos quais a China seja signatária, ou cumprir outras condições estabelecidas por leis e regulamentos. Além de satisfazer um desses critérios, o gestor é obrigado a informar o indivíduo sobre detalhes cruciais da transferência – como a identidade do destinatário no exterior, o propósito do processamento e os tipos de

⁷⁴ Capítulo IV – Direitos dos indivíduos em atividades de tratamentos de informações pessoais.

⁷⁵ Artigo 28.

⁷⁶ Artigo 11.

⁷⁷ Artigo 4. **EUROPEAN UNION**. *General Data Protection Regulation (GDPR)*. Disponível em: <https://gdpr-info.eu/>. Acesso em: 06 maio 2025.

⁷⁸ Artigos 20 e 21. **THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA**. *Personal Information Protection Law of the People's Republic of China*. Disponível em: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm>. Acesso em: 06 maio 2025.

⁷⁹ Artigo 40.

dados a serem transferidos – e, crucialmente, obter o consentimento individual e separado para cada transferência.⁸⁰

No que se refere às sanções administrativas, a Lei prevê multas podem atingir até 5% do faturamento anual, limitadas a 50 milhões de yuans, além de responsabilidade pessoal para indivíduos diretamente envolvidos em violações.⁸¹ Ademais, o Ministério Público chinês, organizações que representam os consumidores ou demais órgãos determinados pela Administração do Ciberespaço da China possuem a legitimidade para propor ações judiciais em defesa dos direitos dos titulares de dados,⁸² conferindo à proteção de informações pessoais um aspecto de interesse público.

Finalmente, cabe frisar que, apesar da lei ser aplicável também ao setor privado, ela prevê um regime sancionatório e de fiscalização diferenciado para as potenciais violações perpetradas por agentes governamentais: quando um órgão estatal falha em cumprir suas obrigações, a penalidade inicial é uma ordem de correção emitida por seus superiores. Além disso, os funcionários diretamente responsáveis também podem ser sancionados de acordo com a lei.⁸³

4. Rumo ao “Efeito Pequim”

Como frisamos ao longo deste artigo, a China vem se consolidando como um ator estratégico na governança global da informação, marcando sua abordagem com algumas características chinesas extremamente peculiares. Esse processo decorre da formulação de um modelo institucional e regulatório próprio, no qual os dados são concebidos como ativos essenciais ao desenvolvimento nacional. Tal modelo reflete uma concepção singular chinesa, pautada na soberania (digital) e na instrumentalização dos dados em prol dos objetivos estatais.

Simultaneamente, o governo chinês tem promovido esforços consistentes para internacionalizar sua abordagem à governança e regulação de dados, mediante instrumentos normativos e iniciativas diplomáticas multilaterais, buscando legitimar sua estratégia de dados como paradigma global.

Essa seção explora a hipótese de que a estratégia de governança de dados da China está a caminho de desencadear um "Efeito de Pequim" na governança global de dados, influenciando outras nações para além de suas fronteiras. Quatro fatores interrelacionados são identificados como motores dessa crescente influência: a

⁸⁰ Artigos 38 e 39.

⁸¹ Artigo 66.

⁸² Artigo 70.

⁸³ Artigo 68.

liderança da China na promoção da cibersegurança e da soberania digital, o sucesso de sua abordagem voltada a considerar dados como fator de produção, a instrumentalização do seu poder infraestrutural através da Rota da Seda Digital e a promoção ativa de seu modelo por meio de iniciativas globais.

A cibersegurança e a soberania digital constituem conceitos interdependentes,⁸⁴ cuja articulação produz efeitos recíprocos de reforço institucional. A cibersegurança, entendida como o conjunto de práticas e instrumentos destinados à análise contínua de sistemas para identificação de vulnerabilidades, mitigação de riscos e prevenção de incidentes cibernéticos, fornece a base técnica e operacional para a proteção da infraestrutura informacional de um Estado. Já a soberania digital, definida como a capacidade de uma entidade de entender, desenvolver e regular as tecnologias digitais,⁸⁵ se torna a base da capacidade estatal de exercer autoridade normativa, tecnológica e estratégica sobre os ativos digitais e infraestruturas críticas que sustentam a economia e a administração pública.

Nesse sentido, a eficácia das políticas de soberania digital depende da existência de mecanismos robustos de cibersegurança, sem os quais não é possível garantir controle efetivo, integridade ou resiliência dos sistemas.⁸⁶ Reciprocamente, a cibersegurança só se consolida plenamente quando inserida em um regime soberano capaz de definir padrões, impor obrigações, fiscalizar operadores e dispor de autonomia decisória sobre tecnologias essenciais. Assim, ambos os conceitos não apenas se sobrepõem, mas compõem dimensões complementares de uma mesma arquitetura de governança, voltada a assegurar a segurança, a autonomia e a continuidade das funções estatais na esfera digital.

No âmbito de um contexto geopolítico cada vez mais desafiador, a soberania digital tem se tornado uma aspiração compartilhada por governos em todo o mundo. Historicamente debatida por países como a China, a Rússia e a Índia,⁸⁷ a noção de

⁸⁴ BELLI *et al*, **Cibersegurança**; BELLI; PAULI; COUTO, Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro; JIANG; BELLI (Orgs.), **Digital Sovereignty in the BRICS Countries**.

⁸⁵ BELLI, L.; JIANG, M. Digital sovereignty from the BRICS: Structuring self-determination, cybersecurity, and control. In: BELLI, L.; JIANG, M. (org.). *Digital sovereignty in the BRICS countries*. Cambridge: Cambridge University Press, 2024.

⁸⁶ BELLI; PAULI; COUTO, Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro; BELLI *et al*, **Cibersegurança**.

⁸⁷ A Rússia, a China e outros Estados membros da Organização de Cooperação de Shanghai (SCO – *Shanghai Cooperation Organisation*) publicaram a primeira versão de seu Código de Conduta Internacional para Segurança da Informação em 2011, e o atualizaram em 2024, enfatizando que “autoridade para o policiamento de políticas públicas relacionadas à internet é direito soberano dos Estados”. Veja mais em **International Code of Conduct for Information Security**, Ministry of Foreign Affairs - People's Republic of China, disponível em: <https://www.mfa.gov.cn/eng/wjbj/zjzg_663340/jks_665232/jkxw_665234/202406/t20240606_11405001.html>. Acesso em: 2 ago. 2025; UNITED NATIONS GENERAL ASSEMBLY, **Letter dated 9 January 2015 from the**

soberania digital tem evoluído de um conceito nicho para uma prioridade central nas agendas de autonomia estratégica, inclusive países ocidentais. Exemplo disso é a União Europeia, cuja liderança política tem defendido publicamente a necessidade de alcançar soberania tecnológica em setores críticos.⁸⁸

A China, com sua experiência de décadas na construção e implementação efetiva da soberania como fundamento de suas políticas digitais, é vista por muitos como uma fonte de inspiração em múltiplas áreas, como política industrial, governança da informatização e regulação da cibersegurança, servindo como um modelo de sucesso em pensamento estratégico. Um exemplo evidente, neste sentido, é a responsabilidade individual dos executivos em caso de descumprimento de obrigações de cibersegurança, definida pelo art. 32.5 da Diretiva (UE) 2022/2555 (conhecida como Diretiva NIS 2), e diretamente importada no arcabouço regulatório europeu, e de maneira mais branda no ordenamento brasileiro,⁸⁹ a partir do Artigo 63 da Lei de Cibersegurança chinesa.

Neste contexto, destaca-se que a estratégia de governança de dados da China, que se estende para além da proteção e segurança de dados, está firmemente ancorada na valorização e uso estratégico de dados para o desenvolvimento nacional. As leis chinesas, como a Lei de Proteção de Informações Pessoais e a Lei de Segurança de Dados, como visto, incluem "cláusulas de soberania" que permitem a restrição de transferências de dados internacionais por motivos de segurança, bem como ações retaliatórias contra países que adotem medidas de proteção de dados consideradas discriminatórias, conforme explorado nas seções anteriores. Embora a apropriação formal do conceito possa ser evitada por alguns, a priorização da soberania digital por líderes ocidentais, como a presidente da Comissão Europeia, Ursula von der Leyen,⁹⁰ sugere um reconhecimento tácito da validade da abordagem chinesa.

Outro exemplo de desdobramento do Efeito Pequim, é a inspiração no modelo chinês no que diz respeito aos chamados "*data spaces*" europeus, instituídos por meio do *Data Governance Act* (DGA)⁹¹, aprovado em maio de 2022 e em vigor desde 2023.

Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, [s.l.: s.n., s.d.].

⁸⁸ URSULA VON DER LEYEN, **A Union that strives for more: My agenda for Europe**, [s.l.: s.n., s.d.].

⁸⁹ Uma abordagem semelhante, embora com um tom e consequências mais brandos, é adotada no Brasil pelo Artigo 8º do Programa de Privacidade e Segurança da Informação, estabelecido pela Portaria SGD/MGI Nº 9.511, de 28 de outubro de 2025. Este artigo determina explicitamente que: "À alta administração compete gerir os riscos no âmbito organizacional, fornecer os recursos necessários para assegurar a gestão da privacidade e da segurança da informação [...]"

⁹⁰ Ibid.

⁹¹ Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governança de Dados) (Texto relevante para efeitos do EEE).

O propósito da DGA é definir um marco harmonizado para o compartilhamento de dados entre setores públicos e privados, facilitando a reutilização de dados detidos por entidades públicas, estabelecendo regras para “intermediários de dados” (“*data intermediation services*”), e incentivando o “altruísmo de dados” ou seja, a disponibilização voluntária de dados para fins sociais ou de pesquisa. A inspiração dos *data spaces* europeus nos *data exchanges* chineses é bastante evidente.

Apesar do arcabouço legal da União Europeia não fazer referência explícita às bolsas de dados chinesas, e as duas iniciativas emergirem de fundamentos diferentes – do lado europeu, buscando-se a promoção da interoperabilidade, e do lado chinês, o desenvolvimento soberano –, a similaridade entre os objetivos das duas iniciativas são manifestas. Porém, cabe destacar que, enquanto na China os *data exchanges* constituem uma realidade consolidada há aproximadamente uma década – tendo evoluído para estruturas economicamente relevantes e, em muitos casos, empresas lucrativas com modelos de negócio estáveis e integração direta às estratégias estatais de desenvolvimento tecnológico –, na União Europeia os *data spaces* permanecem um fenômeno incipiente, cujas aplicações práticas são ainda limitadas.

As bolsas de dados chinesas operam em escala, facilitando transações de dados entre setores públicos e privados, colocando em circulação grandes volumes de dados industriais e urbanos e desempenhando papel central no ecossistema digital nacional. Em contraste, os *data spaces* europeus ainda se encontram majoritariamente em fase piloto, com implementação fragmentada e baixa maturidade operacional.

Assim, as recentes evoluções normativas no campo da governança de dados indicam que soluções regulatórias e institucionais desenvolvidas na China passaram a ser objeto de estudo e, em alguns casos, de reprodução parcial por outros Estados e blocos regionais. A consolidação chinesa de mecanismos como a classificação de dados, a criação de mercados regulados para sua circulação, a atuação estatal coordenada entre segurança, inovação e desenvolvimento industrial, bem como a integração entre políticas de proteção de dados, cibersegurança e soberania digital, tem despertado crescente interesse internacional. Embora adotadas em contextos jurídicos e políticos distintos, diversas iniciativas recentes, incluindo modelos de intermediação de dados, regimes de auditoria de riscos sistêmicos e estruturas de certificação, revelam aproximações conceituais com a experiência chinesa, ainda que adaptadas às exigências institucionais locais. Esse movimento sugere que a China se tornou referência relevante na formulação de estratégias regulatórias e de governança de dados em escala global.

O terceiro pilar do crescente “Efeito Pequim” é a Rota da Seda Digital (RSD), o componente digital da Iniciativa do Cinturão e Rota (ICR), ou *Belt and Road*

Initiative (BRI), lançada oficialmente em 2013 pelo presidente Xi Jinping. Inserida nesse contexto, a RSD representa uma vertente estratégica do projeto, voltada à promoção da conectividade digital global por meio do comércio eletrônico, infraestrutura tecnológica e investimentos orientados, e, por extensão, à promoção de sua abordagem de governança de dados.⁹²

A exportação de infraestruturas de hardware e de software por empresas como Huawei, ZTE, Alibaba, Tencent e ByteDance desempenham papel crucial como motor desse processo.⁹³ Essas infraestruturas digitais exercem um papel regulatório significativo, moldando os ambientes digitais que sustentam. O papel central dessas empresas no fornecimento de cabos submarinos, redes 5G, servidores em nuvem, plataformas de comércio eletrônico e soluções de Internet das Coisas (IoT) permite a implementação de normas "autoexecutáveis" por meio do design arquitetônico de suas tecnologias. Essa dinâmica, que mobiliza o que a cientista política Susan Strange definiu como "poder estrutural",⁹⁴ permite que a soberania nacional da China seja estendida globalmente por procuração, desde que as empresas não sejam efetivamente regulamentadas pelos países onde operam. Isso distingue o "Efeito de Pequim" do "Efeito de Bruxelas", que é impulsionado principalmente pela transplantação de políticas,⁹⁵ enquanto o modelo chinês também se propaga por meio da tecnologia e da ordem privada. Assim, ao expandir sua rede de parcerias comerciais e sua capacidade de conectividade, a China não só está apenas exportando seus produtos e serviços digitais, mas também está pronta para projetar seu poder brando (*soft power*) e promover uma imagem mais positiva dos valores e do sistema de governança que vem construindo ao longo das últimas décadas.⁹⁶

O quarto fator determinante da estratégia de governança de dados da China é a intenção explícita do governo chinês de promover seu sistema normativo e institucional como um modelo global bem-sucedido. Essa faceta da internacionalização é buscada de forma metódica por meio de uma variedade de

⁹² PAUL TRILOLO *et al*, *The Digital Silk Road: Expanding China's Digital Footprint*, Eurasia Group, 2020. DEKKER, Brigitte; OKANO-HEIJMANS, Maaïke; ZHANG, Eric Siyi, *Unpacking China's Digital Silk Road*, [s.l.]: Clingendael Institute, 2020.

⁹³ HILLMAN, Jonathan E., *The Digital Silk Road: China's quest to wire the world and win the future*, Paperback edition. London: Profile Books Ltd, 2022.

⁹⁴ STRANGE, Susan, *States and markets: an introduction to international political economy*, 1. publ. in the United States. New York: Blackwell, 1988.

⁹⁵ BRADFORD, Anu, *The Brussels effect: how the European Union rules the world*, New York: Oxford University Press, 2020.

⁹⁶ JIANGYU WANG, *China's Governance Approach to the Belt and Road Initiative (BRI): Partnership, Relations, and Law*, *Forthcoming in Global Trade and Customs Journal*, Vol. 14, Issue 5, May 2019., n. NUS Law Working Paper No. 2019/005, 2019.

iniciativas intergovernamentais e diplomáticas.⁹⁷ Desde o anúncio da ICR em 2013, o governo chinês tem a complementado com projetos globais ambiciosos que incluem a Iniciativa de Desenvolvimento Global (IDG), a Iniciativa de Segurança Global (ISG)⁹⁸ e a Iniciativa de Civilização Global (ICG).⁹⁹

Essas iniciativas, embora não se concentrem exclusivamente em questões digitais, atribuem a elas um papel transversal e significativo. A IDG, por exemplo, busca alinhar o conceito de governança de desenvolvimento da China com os Objetivos de Desenvolvimento Sustentável da ONU, com a economia digital e a conectividade sendo uma de suas oito áreas prioritárias.¹⁰⁰ De maneira semelhante, a ISG propõe uma reforma da segurança coletiva com foco no ciberespaço como um de seus seis pilares.¹⁰¹ Esses projetos demonstram o compromisso do governo chinês em posicionar seu modelo de governança como uma opção válida, especialmente para países em desenvolvimento.

Destarte, a atual estratégia de governança de dados da China representa uma elaboração sofisticada de políticas industriais e estrangeiras que outrora já sustentaram a supremacia tecnológica dos EUA. As grandes empresas de tecnologia chinesas exercem uma soberania privada que acaba por estender a soberania do estado chinês por procuração, afirmando a influência chinesa globalmente por meio de laços comerciais e tecnológicos. Essa estratégia, portanto, não é apenas um plano de desenvolvimento interno, mas um motor de projeção de poder internacional que busca promover um novo modelo de governança digital global.

Conclusão

O presente artigo analisou o modelo de governança de dados da China como uma abordagem sistêmica e multifacetada, centrada na eficiência, na segurança nacional e no desenvolvimento tecnológico, em contraste com os paradigmas

⁹⁷ **A New Model of International Relations**, China.org, disponível em: <http://www.china.org.cn/english/china_key_words/2016-03/01/content_37907319.html>. Acesso em: 2 ago. 2025.

⁹⁸ XINHUA, Xi proposes Global Security Initiative, **The National Committee of the Chinese People's Political Consultative Conference**.

⁹⁹ **Global Civilization Initiative**, China Diplomacy, disponível em: <http://en.chinadiplomacy.org.cn/2024-05/11/content_117181406.shtml>. Acesso em: 2 ago. 2025.

¹⁰⁰ MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA (GOVERNMENT), **Global Development Initiative-Building on 2030 SDGs for Stronger, Greener and Healthier Global Development**, United Nations Department of Economic and Social Affairs, disponível em: <<https://sdgs.un.org/partnerships/global-development-initiative-building-2030-sdgs-stronger-greener-and-healthier-global>>. Acesso em: 2 ago. 2025.

¹⁰¹ CHINESE GOVERNMENT, **The Global Security Initiative Working Paper**, disponível em: <http://en.chinadiplomacy.org.cn/pdf/The_Global_Security_Initiative_Concept_Paper.pdf>. Acesso em: 2 ago. 2025.

ocidentais focados na proteção de direitos individuais. O estudo demonstrou como essa estratégia se fundamenta em elementos históricos e culturais, utilizando mecanismos como a experimentação normativa e a regulação facilitadora para alinhar a legislação (como a Lei de Cibersegurança, a Lei de Segurança de Dados e a Lei de Proteção de Informações Pessoais) com as políticas industriais e planos estratégicos do Estado, a fim de consolidar a soberania digital e o protagonismo tecnológico do país.

A emergência do "Efeito Pequim", um fenômeno no qual a China projeta seu modelo de governança de dados globalmente, ganha destaque e necessidade de compreensão por meio de uma análise holística das práticas que consolidam a estratégia da China em relação à governança de dados. Como visto, essa projeção ocorre não apenas por meio de sua influência normativa, mas também pela exportação de infraestrutura e tecnologia digital por meio da Rota da Seda Digital. Diferentemente do "Efeito Bruxelas", a estratégia de governança de dados chinesa se propaga pelo *design* arquitetônico de suas tecnologias, operando como uma forma de "poder estrutural" capaz de influenciar e moldar ambientes digitais em outros países.

Em suma, a estratégia de governança de dados chinesa representa um paradigma alternativo que desafia as normas euro-americanas de governança de dados. A crescente influência da China, especialmente no Sul Global, sugere que seu modelo pode se tornar uma referência para outros países, reconfigurando as discussões e práticas internacionais sobre regulação digital.

Referências Bibliográficas

ARCESATI, Alex He, Rebecca. **Data Marketplaces and Governance: Lessons from China**. Centre for International Governance Innovation. Disponível em: <<https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>>. Acesso em: 5 dez. 2025.

BELLI, Luca; FRANQUEIRA, Bruna Diniz; BAKONYI, Erica; *et al.* **Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano**. Rio de Janeiro, RJ: FGV Direito Rio, 2023. Disponível em: <<https://hdl.handle.net/10438/33784>>.

BELLI, Luca; GASPAR, Walter B; COUTO, Natalia; *et al.* **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**. RIO DE JANEIRO, RJ: Lumen Juris, 2026.

BELLI, Luca; PAULI, Breno; COUTO, Natália. Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro. **Governança da cibersegurança no Brasil: entender o passado, esclarecer o presente e construir o futuro**, Disponível em: <<https://cyberbrics.info/wp-content/uploads/2024/06/PP-CTS-FGV-Ciberseguranca.pdf>>. Acesso em: 3 dez. 2024.

BRADFORD, Anu. *The Brussels effect: how the European Union rules the world*. New York: Oxford University Press, 2020.

CHANG, Amy. *Warring State: China's Cybersecurity Strategy*. **Center for a New American Security**, 2014. Disponível em: <https://www.files.ethz.ch/isn/186337/CNAS_WarringState_Chang.pdf>. Acesso em: 1 dez. 2025.

CHEN, Qiheng. China's new National Data Bureau: what it is and what it is not. Disponível em: <<http://thechinaproject.com/2023/03/20/chinas-new-national-data-bureau-what-it-is-and-what-it-is-not/>>. Acesso em: 8 maio 2025.

CHINESE GOVERNMENT. **The Global Security Initiative Working Paper**. Disponível em: <http://en.chinadiplomacy.org.cn/pdf/The_Global_Security_Initiative_Concept_Paper.pdf>. Acesso em: 2 ago. 2025.

CREEMERS, Rogier. China's Cyber Governance Institutions. **Leiden Asia Centre**, v. January 2021, 2021. Disponível em: <<https://leidenasiacentre.nl/wp-content/uploads/2021/01/Chinas-Cyber-Governance-Institutions-Layout-geconverteerd-1.pdf>>. Acesso em: 8 maio 2025.

CREEMERS, Rogier. China's emerging data protection framework. **Journal of Cybersecurity**, v. 8, n. 1, 2022. Disponível em: <<https://doi.org/10.1093/cybsec/tyac011>>. Acesso em: 12 maio 2025.

Versão pre-print de Belli, L., & Chang, S. (2026). Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira De Direitos Fundamentais & Justiça*, 24(53). <https://doi.org/10.30899/dfj.v24i53.1730>

CREEMERS, Rogier; WEBSTER, Graham; TRIOLO, Paul. **Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)**. Stanford University DigiChina. Disponível em: <<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>>. Acesso em: 6 out. 2022.

DEKKER, Brigitte; OKANO-HEIJMANS, Maaïke; ZHANG, Eric Siyi. **Unpacking China's Digital Silk Road**. [s.l.]: Clingendael Institute, 2020. (Unpacking China's Digital Silk Road). Disponível em: <<https://www.jstor.org/stable/resrep25693.1>>. Acesso em: 2 ago. 2025.

ERIE, Matthew S; STREINZ, Thomas. The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance. **N.Y.U. J. Int'l L. & Pol.**, v. 1, n. 54, p. 61, 2022.

GAO, Bai; RU, Yi. Industrial Policy and Competitive Advantage: A Comparative Study of the Cloud Computing Industry in Hangzhou and Shenzhen. *In: Innovation and China's Global Emergence*. [s.l.: s.n.], 2021. Disponível em: <<https://epress.nus.edu.sg/innovationandchina/chapterten/>>. Acesso em: 10 jan. 2025.

HEILMANN, Sebastian. Policy Experimentation in China's Economic Rise. **Studies in Comparative International Development**, v. 43, n. 1, p. 1–26, 2008.

HEILMANN, Sebastian. **Red Swan: How Unorthodox Policy-Making Facilitated China's Rise**. [s.l.]: The Chinese University Press, 2018. Disponível em: <<http://www.jstor.org/stable/10.2307/j.ctv2n7q6b>>. Acesso em: 7 maio 2025.

HILLMAN, Jonathan E. **The Digital Silk Road: China's quest to wire the world and win the future**. Paperback edition. London: Profile Books Ltd, 2022.

HULD, Arendse. Cross-Border Data Transfer - New Measures for Security Review. Disponível em: <<https://www.china-briefing.com/news/cross-border-data-transfer-new-measures-offer-clarification-on-security-review/>>. Acesso em: 2 ago. 2025.

HULD, Arendse. Shenzhen Data Regulations: Clear Limits Imposed on Businesses. Disponível em: <<https://www.china-briefing.com/news/shenzhen-new-data-regulations-explained-impact-china-personal-data-protection/>>. Acesso em: 7 maio 2025.

JIANG, Min. A brief prehistory of China's social credit system. **Communication and the Public**, v. 5, n. 3–4, p. 93–98, 2020.

JIANG, Min; BELL, Luca (Orgs.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**. Cambridge: Cambridge University Press, 2025. (Communication, Society and Politics). Disponível em: <<https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/27E9FD7E4579C76C8D4BA52F7670B431>>. Acesso em: 2 ago. 2025.

Versão pre-print de Belli, L., & Chang, S. (2026). Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira De Direitos Fundamentais & Justiça*, 24(53). <https://doi.org/10.30899/dfj.v24i53.1730>

JIANGYU WANG. China's Governance Approach to the Belt and Road Initiative (BRI): Partnership, Relations, and Law. **Forthcoming in Global Trade and Customs Journal, Vol. 14, Issue 5, May 2019.**, n. NUS Law Working Paper No. 2019/005, 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3346427>. Acesso em: 2 ago. 2025.

LU, Julia. Data exchanges in China, explained · TechNode. Disponível em: <<https://technode.com/2021/08/17/chinas-data-exchanges-explained/>>. Acesso em: 5 dez. 2025.

LUONG, Ngor; ARNALD, Zachary; MURPHY, Ben. **Understanding Chinese Government Guidance Funds: An Analysis of Chinese-Language Sources.** [s.l.]: Center for Security and Emerging Technology, 2021. (CSET Issue Brief). Disponível em: <<https://cset.georgetown.edu/publication/understanding-chinese-government-guidance-funds/>>. Acesso em: 8 maio 2025.

MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA (GOVERNMENT). **Global Development Initiative-Building on 2030 SDGs for Stronger, Greener and Healthier Global Development.** United Nations Department of Economic and Social Affairs. Disponível em: <<https://sdgs.un.org/partnerships/global-development-initiative-building-2030-sdgs-stronger-greener-and-healthier-global>>. Acesso em: 2 ago. 2025.

MOST (MINISTRY OF SCIENCE AND TECHNOLOGY). **Governance Principles for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence.** China Daily. Disponível em: <<https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html>>. Acesso em: 8 maio 2025.

OOIJEN, Charlotte van; UBALDI, Barbara; WELBY, Benjamin. **A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance.** Paris: OECD, 2019. (OECD Working Papers on Public Governance). Disponível em: <https://www.oecd.org/en/publications/a-data-driven-public-sector_09ab162c-en.html>. Acesso em: 7 maio 2025.

PAUL TRIOLO; KEVIN ALLISON; CLARISE BROWN; *et al.* The Digital Silk Road: Expanding China's Digital Footprint. **Eurasia Group**, 2020. Disponível em: <<https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint.pdf>>. Acesso em: 2 ago. 2025.

PERNOT-LEPLAY, Emmanuel. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? **Penn State Journal of Law & International Affairs**, 2020.

Versão pre-print de Belli, L., & Chang, S. (2026). Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira De Direitos Fundamentais & Justiça*, 24(53). <https://doi.org/10.30899/dfj.v24i53.1730>

RIHUI, Ouyang. Data as a Factor of Production Promoting the Deep Integration of the Digital Economy and the Real Economy: Theoretical Logic and Analysis Framework. **Frontiers of Economics in China**, v. 19, n. 2, p. 129–153, 2024.

ROGIER CREEMERS. [INTERVIEW] "The Chinese approach to digital sovereignty": 4 questions to Rogier Creemers – Sciences Po Chair Digital, Governance and Sovereignty. Disponível em: <<https://www.sciencespo.fr/public/chaire-numerique/en/2023/04/05/interview-the-chinese-approach-to-digital-sovereignty/>>. Acesso em: 2 ago. 2025.

STRANGE, Susan. **States and markets: an introduction to international political economy**. 1. publ. in the United States. New York: Blackwell, 1988.

THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA. Personal Information Protection Law of the People's Republic of China. Disponível em: <http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm>. Acesso em: 12 maio 2025.

UNITED NATIONS GENERAL ASSEMBLY. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. [s.l.: s.n., s.d.]. Disponível em: <<https://documents.un.org/doc/undoc/gen/n15/014/02/pdf/n1501402.pdf>>. Acesso em: 2 ago. 2025.

URSULA VON DER LEYEN. **A Union that strives for more: My agenda for Europe**. [s.l.: s.n., s.d.]. Disponível em: <https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf>. Acesso em: 2 ago. 2025.

U.S. CHAMBER OF COMMERCE. **Made in China 2025: Global Ambitions Built on Local Protections**. [s.l.]: U.S. Chamber of Commerce, 2017. Disponível em: <<https://www.uschamber.com/international/made-china-2025-global-ambitions-built-local-protections-0>>. Acesso em: 7 maio 2025.

WANG, Wayne Wei. China's digital transformation: Data-empowered state capitalism and social governmentality. **The African Journal of Information and Communication (AJIC)**, n. 31, 2023. Disponível em: <<https://ajic.wits.ac.za/article/view/16296>>. Acesso em: 2 ago. 2025.

WANG, Wayne Wei. Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China. **Computer Law & Security Review**, v. 55, p. 106030, 2024.

WEBSTER, Graham; CREEMERS, Rogier; KANIA, Elsa; *et al.* Full Translation: China's "New Generation Artificial Intelligence Development Plan" (2017). Disponível em:

Versão pre-print de Belli, L., & Chang, S. (2026). Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira De Direitos Fundamentais & Justiça*, 24(53). <https://doi.org/10.30899/dfj.v24i53.1730>

<<https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>>. Acesso em: 8 maio 2025.

WHITMAN, Christina. Privacy in Confucian and Taoist Thought. *In*: D. MUNRO (Org.). **Individualism and Holism: Studies in Confucian and Taoist Values**. Ann Arbor: Univ. of Michigan: Center for Chinese Studies, 1985. Disponível em: <https://repository.law.umich.edu/book_chapters/21>.

XINHUA. Xi proposes Global Security Initiative. **The National Committee of the Chinese People's Political Consultative Conference**, Disponível em: <http://en.cppcc.gov.cn/2022-04/21/c_745515.htm>. Acesso em: 2 ago. 2025.

ZHU, Huang. Shenzhen Issues First Comprehensive Data Rules. Disponível em: <<https://www.chinatrademonitor.com/shenzhen-issues-first-comprehensive-data-rules/>>. Acesso em: 7 maio 2025.

中华人民共和国国务院令. **网络数据安全条例_信息产业（含电信）**. 中国政府网. Disponível em: <https://www.gov.cn/zhengce/content/202409/content_6977766.htm>. Acesso em: 12 maio 2025.

页之码. Hangzhou introduces new policies to vigorously support the development of cross-border e-commerce. Disponível em: <<https://yezshimaip.com/en/article/2023-02/1675872206735.html>>. Acesso em: 18 nov. 2024.

A New Model of International Relations. China.org. Disponível em: <http://www.china.org.cn/english/china_key_words/2016-03/01/content_37907319.html>. Acesso em: 2 ago. 2025.

China unveils guideline on improving market-based allocation of production factors. Disponível em: <https://english.www.gov.cn/policies/latestreleases/202004/10/content_WS5e8faa09c6d0c201c2cc0922.html?utm_source=chatgpt.com>. Acesso em: 5 dez. 2025.

Decision of the Fourth Plenum of the 19th Central Committee of the Chinese Communist Party. Disponível em: <<https://interpret.csis.org/translations/decision-of-the-fourth-plenum-of-the-19th-central-committee-of-the-chinese-communist-party/>>. Acesso em: 5 dez. 2025.

Full Text of Jiang Zemin's Report at the 16th Party Congress. China Through a Lens. Disponível em: <<http://www.china.org.cn/english/2002/Nov/49107.htm>>. Acesso em: 7 maio 2025.

Full Text: Report on the Work of the Government (2015). The State Council of the People's Republic of China. Disponível em:

Versão pre-print de Belli, L., & Chang, S. (2026). Governança de dados na China: Soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira De Direitos Fundamentais & Justiça*, 24(53). <https://doi.org/10.30899/dfj.v24i53.1730>

<https://english.www.gov.cn/archive/publications/2015/03/05/content_281475066179954.htm>. Acesso em: 8 maio 2025.

Global Civilization Initiative. China Diplomacy. Disponível em: <http://en.chinadiplomacy.org.cn/2024-05/11/content_117181406.shtml>. Acesso em: 2 ago. 2025.

Implementation of "Internet Plus Regulation" in Safety Production Precise Law Enforcement in the City's Industrial and Mining Fields. Window of Yiwu - Free Trade. Disponível em: <https://www.yw.gov.cn/art/2024/4/21/art_1229436709_59477522.html>. Acesso em: 8 maio 2025.

Information security technology— Personal information (PI) security specification - GB/T 35273—2020 (Replacing GB/T 35273-2017). Disponível em: <<https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>>. Acesso em: 11 out. 2022.

International Code of Conduct for Information Security. Ministry of Foreign Affairs - People's Republic of China. Disponível em: <https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/jkxw_665234/202406/t20240606_11405001.html>. Acesso em: 2 ago. 2025.

"Performance Legitimacy" and China's Political Adaptation Strategy. CoLab. Disponível em: <<https://colab.ws/articles/10.1007%2Fs11366-011-9140-8>>. Acesso em: 7 maio 2025.

Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) (Texto relevante para efeitos do EEE). Disponível em: <<http://data.europa.eu/eli/reg/2022/868/oj>>. Acesso em: 5 dez. 2025.