COMPETITION AND DATA PROTECTION IN THE DIGITAL ECONOMY: A COMPARATIVE ANALYSIS OF THE EU AND CHINA

ARLETTA GORECKA*

TABLE OF CONTENTS

* Arletta Gorecka, Ph.D., University of Strathclyde, Glasgow, UK, Lecturer in Law, Glasgow International College, Glasgow, UK.

COMPETITION AND DATA PROTECTION IN THE DIGITAL ECONOMY: A COMPARATIVE ANALYSIS OF THE EU AND CHINA

Arletta Gorecka*

Abstract:
This article conducts a comparative analysis of competition law and data protection frameworks in China and the European Union, examining how each jurisdiction regulates digital markets, governs personal data, and projects regulatory influence globally. Drawing on China's Anti-Monopoly Law (AML), the Personal Information Protection Law (PIPL), as well as the EU's Articles 101 and 102 TFEU and the General Data Protection Regulation (GDPR), the study contrasts the underlying philosophies, institutional designs, enforcement styles, and cross-border implications of the two regulatory systems. It highlights that China's regulatory model integrates competition policy with national security and industrial objectives, while the EU's frameworks prioritize market integration and the protection of individual rights. Comparative case studies of digital platforms, involving major technology firms, such as Alibaba, Tencent, Google, Meta, and Didi, demonstrate how each framework operates in practice and how enforcement increasingly intersects with questions of digital sovereignty. The article further assesses the extraterritorial reach of these regimes, the sustainability of the "Brussels Effect" considering recent EU proposals to simplify GDPR rules, and the emergence of a "Beijing Effect" shaped through data localisation mandates and Digital Silk Road initiatives. The conclusion synthesizes areas of divergence and limited convergence, arguing that China and the EU represent two influential yet competing models of digital governance whose interaction will shape the future of global regulatory order.

Keywords: privacy, data protection, big data, competition law

1. INTRODUCTION

A. BACKGROUND AND SIGNIFICANCE

Competition law and data protection have become two of the most influential regulatory regimes shaping the global digital economy. Both China and the European Union (EU) have rapidly developed comprehensive legal frameworks to govern digital markets, reflecting their growing concern about platform power,

* Arletta Gorecka, Ph.D., University of Strathclyde, Glasgow, UK, Lecturer in Law, Glasgow International College, Glasgow, UK.

cross-border data flows, and the societal impact of large technology firms. China's regulatory environment has undergone significant consolidation since 2018, culminating in the revised Anti-Monopoly Law (AML, amended 2022) and the enactment of the Personal Information Protection Law (PIPL, 2021). In the EU, competition law continues to be grounded in Articles 101 and 102 TFEU and the EU Merger Regulation, while data protection has been transformed by the General Data Protection Regulation (GDPR, 2018), reinforced by ongoing reforms and simplification proposals introduced in 2024–2025.[1]

Across both systems, enforcement responsibilities are entrusted to powerful national and supranational authorities, notably China's State Administration for Market Regulation (SAMR) and Cyberspace Administration of China (CAC), and the EU's Directorate-General for Competition (DG Competition) and national Data Protection Authorities (DPAs). The combination of strong institutional capacity, expanding legal mandates, and heightened political interest has made both jurisdictions central actors in global regulatory debates.[2]

B. THEORETICAL FRAMING: BRUSSELS EFFECT AND BEIJING EFFECT

This article situates the comparison of Chinese and EU regulatory models within two influential theoretical frameworks: the Brussels Effect and the emerging Beijing Effect.[3]

The Brussels Effect, first conceptualised by Anu Bradford, refers to the EU's ability to externalise its regulatory standards beyond its borders through market mechanisms, legal extraterritoriality, and the global reach of multinational firms.[4] GDPR, EU antitrust enforcement, and data-transfer adequacy decisions have become widely cited examples of how EU rules can shape global practices even without formal international

---

[1] Fan Longduan Fa (反垄断法) [Anti-Monopoly Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 30, 2007, effective Aug. 1, 2008) (China); Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China); Treaty on the Functioning of the European Union arts. 101–102, 2008 O.J. (C 115) 88–89.; Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

[22] Jialiang Zhu & Jinnan Gu, *Intensified law enforcement and firm innovation: Evidence from China's antitrust consolidation*, CHINA ECONOMIC REVIEW, Oct., 2024 at 1. Pablo Ibáñez Colomo, *The (Second) Modernisation of Article 102 TFEU: Reconciling Effective Enforcement, Legal Certainty and Meaningful Judical Review*, JOURNAL OF EUROPEAN COMPETITION LAW & PRACTICE, Nov. 13, 2023, at 608.

[3] Ivanova Yordanka, *The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World in* vol.13, DATA PROTECTION AND ARTIFICIAL INTELLIGENCE (Oxford: Hart Publishing, 2020);
Graham Greenleaf, *China's Completed Personal Information Protection Law: Rights Plus Cyber-security*, PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, Dec. 27, 2021, at 20.

[4] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD, (2020).

agreements.

In parallel, scholars and policy analysts have begun to identify what can be described as a Beijing Effect, a phenomenon through which China exports elements of its digital governance model, particularly data localisation, cybersecurity review mechanisms, and infrastructure-embedded regulatory norms. This diffusion occurs through initiatives such as the Digital Silk Road, through outbound investment by Chinese technology companies, and through the global incorporation of Chinese technical standards.[5]

Integrating these frameworks provides a conceptual lens for examining how China and the EU compete in shaping international norms for data governance and digital market regulation.

C. Scope, Methodology, and Temporal Context

This article analyses the legal frameworks and enforcement practices of China and the EU in the period 2018-2025, a timeframe during which both jurisdictions significantly expanded and restructured their digital regulatory architecture. For China, this includes the strengthened AML enforcement campaign beginning in 2018, the 2021 PIPL, the 2021–2023 cross-border data transfer regulations, and the 2022 AML amendments. For the EU, the analysis covers GDPR enforcement developments since 2018, recent EU competition decisions and digital-market cases, and the European Commission's 2024-2025 proposals to streamline aspects of GDPR implementation.

The methodology is comparative and doctrinal, focusing on statutory provisions, regulatory guidance, enforcement actions, and landmark cases involving major technology firms such as Alibaba, Tencent, Google, Meta, and Didi. The article also draws on institutional documents, policy statements, and scholarly literature related to digital sovereignty, antitrust theory, and data protection.

Through this framework, the article evaluates how China and the EU define and enforce competition and data protection rules, how they project regulatory influence extraterritorially, and how their differing regulatory philosophies, one emphasising stronger state coordination and the other emphasising market integration and individual rights, shape the evolving global regulatory landscape.

II. Regulatory Foundations in China and the EU

A. Competition Law Frameworks

[5] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance*, New York University Journal of International Law and Politics, Mar. 23, 2021 at 1.

1. China's Competition Law and Enforcement

China's competition regime is grounded in the 2008 Anti-Monopoly Law (AML) of the People's Republic of China, and most recently amended in 2022 to address new challenges posed by digital markets and platform-based economies.[6] Article 1 of the AML declares its purpose as to limit anti-competitive practices, uphold fair market conditions, improve economic performance, and safeguard the interests of consumers and society at large.[7] The AML prohibits the same three categories as Western antitrust laws: (1) monopolistic agreements (cartels); (2) abuse of a dominant market position (akin to Article 102 TFEU); and (3) concentrations of undertakings (merger control) that may eliminate or restrict competition.[8] Yet, unlike in Western systems, these prohibitions operate within a governance framework that places the state at the centre of market ordering. Article 2 of the AML explicitly gives it extraterritorial scope: it applies not only to conduct within China, but also to conduct outside China "which serves to eliminate or restrict competition within the domestic market of China".

A distinctive feature of China's AML is its explicit regulation of administrative monopolies and government-led distortions. Articles 9 and 10 establish the Anti-Monopoly Commission under the State Council, responsible for overall coordination and policy guidance, and delegate enforcement powers to the State Administration for Market Regulation (SAMR) and corresponding local authorities. This dual structure ensures vertical control and policy coherence but also embeds competition enforcement within the administrative hierarchy of the state. Notably, Article 7 explicitly exempts or provides special treatment for "lifeline" industries critical to national economic security, such as energy, telecommunications, and transport, acknowledging the state's continuing role in maintaining public monopolies or oligopolies in strategic sectors. This provision illustrates the interaction between market mechanisms and state regulatory objectives within China's system in which anti-monopoly policy serves both to promote efficiency and to reinforce the overarching framework of China's state-guided market economy.

Enforcement under the AML is managed by the State Administration for Market Regulation (SAMR) and operates through a centralised structure at the national level and a network of provincial and municipal branches. This institutional design

---

[6] Fan Longduan Fa (反垄断法) [Anti-Monopoly Law], (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 30, 2007, effective Aug. 1, 2008) (China).

[7] Bruce M. Owen, Su Sun & Wentong Zheng, *China's Competition Policy Reforms: The Anti-Monopoly Law and Beyond*, ANTITRUST LAW JOURNAL, 2008, at 231.

[8] Yong Huang, Shan Jiang, Diana L. Moss & Randy Stutz, *China's 2007 Anti-Monopoly Law: Competition and the Chinese Petroleum Industry*, ENERGY LAW JOURNAL, 2010 at 337.

allows the central government to set uniform enforcement priorities while enabling localised investigations that reflect regional market dynamics.[9] The AML grants SAMR extensive investigatory powers and access business data and electronic communications. Penalties for violations are significant: firms found to have engaged in monopolistic conduct may face fines of up to 10% of their turnover from the preceding financial year, while individuals and responsible managers can also face personal liability. Although the vast majority of mergers receive unconditional clearance (roughly 98%), transactions involving sensitive industries, foreign ownership, or digital platform effects tend to attract deeper scrutiny. In practice, Chinese enforcement has grown especially vigorous in the digital economy: since about 2018 SAMR has pursued tech platforms for abuses of dominance and anti-competitive agreements.[10] The highest-profile enforcement action to date was the April 2021 penalty against Alibaba. SAMR found that the company had abused its dominant position in China's online retail platform market by requiring merchants to choose between Alibaba and rival platforms, a practice known as "er xuan yi" ("pick one of two").[11] The regulator concluded that this conduct excluded competitors, restricted merchant choice, and harmed consumers through reduced platform diversity and innovation. Alibaba was fined RMB 18.2 billion (approximately USD 2.8 billion), equivalent to 4% of its 2019 domestic sales. SAMR's analysis resembled EU Cartel scrutiny: it defined a relevant market (platform commerce), established Alibaba's dominant share, and found harm to retailers and consumers from exclusionary "pick one of two" platform rules.[12]

The Alibaba case marked a turning point in Chinese competition enforcement. It demonstrated SAMR's willingness to apply sophisticated analytical tools, such as market definition and dominance assessment familiar from EU and U.S. practice, while situating enforcement within China's broader regulatory and policy framework.[13] The case functioned not only as an antitrust precedent but also as an instrument of industrial regulation, signalling to other technology giants that dominance in digital ecosystems must align with state-defined policy objectives and regulatory priorities.[14] Subsequent actions against companies like Meituan, Tencent, and Didi reinforced this pattern, illustrating

---

[9] Yu Scott (余昕刚), China Proposes to Fine Tune Its Anti-Monopoly Law, Zhong Lun Law Firm, Feb 9, 2020), https://en.zhonglun.com/research/articles/27091.html, (last visited Nov. 7, 2025).
[10] *Ibid.*
[11] Sandra Marco Colino, *The Case Against Alibaba in China and Its Wider Policy Repercussion*, JOURNAL OF ANTITRUST ENFORCEMENT, Mar., 2022 at 217.,
[12] *Ibid.*
[13] See Sandra Marco Colino, *The Incursion of Antitrust into China's Platform Economy*, ANTITRUST BULLETIN, Jun., 2022 at 237.
[14] *Ibid.*

how AML enforcement operates at the intersection of market discipline and state macroeconomic control.[15]

Historically, Chinese enforcement focused more on cartels and state monopolies, but in recent years SAMR has targeted platform gatekeepers. In the years immediately following the AML16's enactment, enforcement activity primarily involved traditional price-fixing and resale price maintenance cases, often in manufacturing and consumer goods sectors. These early cases served an educational function, signalling to domestic enterprises that China's competition regime would be applied with increasing rigour. In 2020-2022 SAMR investigated and fined (often for abuse of dominance) major Chinese tech companies beyond Alibaba.[17]This period marked the maturation of Chinese competition enforcement, with regulators demonstrating greater sophistication in defining relevant markets, assessing data-related competitive advantages, and addressing algorithmic or exclusivity-based abuses. For instance, the penalties imposed on Meituan for exclusivity practices and Tencent for unnotified concentrations showed SAMR's growing willingness to apply nuanced economic analysis to platform ecosystems.[18] Private antitrust litigation remains rare, but the 2022 AML amendments explicitly empower public prosecutors to sue for damages in public interest cases, potentially expanding enforcement beyond administrative penalties.[19] China's competition policy is administered by SAMR and its local branches within China's centralised administrative structure.[20] It integrates market-regulation tools with wider economic and regulatory priorities, as seen in its statutory objectives and recent emphasis on "digital ecosystems" and the socialist market model. The resulting framework blurs the traditional boundary between economic law and industrial policy, using competition enforcement not merely to correct market failures but to shape market structure in alignment with national development strategies and long-term political goals.

China's AML is enforced by the State Administration for Market Regulation (SAMR), which subsumed the previous

---

[15] Kenneth Khoo, Sinchit Lai & Chuyue Tian, *The Impact of Antitrust Enforcement on China's Digital Platforms: Evidence from SAMR v Alibaba*,„INTERNATIONAL REVIEW OF LAW AND ECONOMICS, Sept., 2025.

16 Jing Wang, *Sustainability of China's Anti- Monopoly Law in the Digital Era: An Observation on the "Choosing One from Two" Jurisprudence from China,* In: 19th Asian Law Institute Conference, 2022-05-28 - 2022-05-29, University of Tokyo.

[17] O'Melveny & Myers LLP, *China Competition & Trade Review* (Mar. 30, 2022) https://www.omm.com/insights/alerts-publications/china-competition-trade-review-issue-6-march-2022./

[18] Kenneth Khoo et al., *The Impact of Antitrust Enforcement on China's Digital Platforms: Evidence from SAMR v Alibaba* ' , INT'L REV. L. & ECON., May. 9, 2025.

[19] Wang Jing & Dermot Cahill, *Legitimacy and effectiveness concerns in China's private antitrust enforcement regime: a comparative analysis with the EU and US regimes*, 11 J. ANTITRUST ENF'T 3, 454 (2023).

[20] Stephanie Wu,'China: Overview, GLOB. Competition REV. (Mar. 19, 2019), https://globalcompetitionreview.com/review/the-asia-pacific-antitrust-review/2019/article/china-overview.

competition agencies (MOFCOM, NDRC, SAIC) during the 2018 administrative reforms.[21] SAMR has regional branches empowered to investigate local cases. SAMR is guided by the State Council's Anti-Monopoly Commission, a policymaking body chaired by high-level officials.[22] In practice, SAMR's enforcement approach often reflects broader regulatory priorities: it may coordinate enforcement in sectors deemed strategically important, and it operates within a regulatory structure ultimately overseen by central political authorities.[23] Private parties may bring antitrust suits in Chinese courts, but such private enforcement has been limited.[24]

2. EU Competition Law and Enforcement

In the EU, competition law is rooted in the EU Treaties. It constitutes one of the cornerstones of the European Union's internal market, designed to ensure that economic integration proceeds based on open and undistorted competition. Articles 101 and 102 of the Treaty on the Functioning of the EU (TFEU) prohibit, respectively, anticompetitive agreements and abuse of a dominant position that affecst trade between Member States.[25] These provisions reflect the dual objective of EU competition law: safeguarding consumer welfare while preserving the free flow of goods and services across national borders.[26] Notably, these provisions are directly applicable and supplemented by secondary legislation. The most significant of these is Regulation 1/2003, which decentralised enforcement by empowering national competition authorities and courts to apply Articles 101 and 102, thereby creating a networked enforcement model across the Union.

Article 101(1) TFEU contains a blanket prohibition on cartels and restrictive agreements within the internal market. It captures a wide range of horizontal and vertical restraints, including price-fixing, market sharing, and output limitation, and is enforced through both administrative fines and private actions for damages.[27] Article 102 TFEU forbids "any abuse by one or more undertakings of a dominant position within the internal market",

---

[21] Liu Zhijin, *Competition Law in China: A Law and Economics Perspective, Jingyuan MA*, CONCURRENCES, Sept. 1, 2020.

[22] Adrian Emch & Wang Xiaoye, *Competition Law 2.0 – Amending China's Anti- Monopoly Law* (Mar. 6, 2021), https://ssrn.com/abstract=3799023.

[23] Wang Jing & Dermot Cahill, supra note 19.

[24] *Ibid.*

[25] Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. (C 115) 47.

[26] Alison Jones & Albertina Albors-Llorens, *The Image(s) of the "Consumer" in EU Competition Law 'in* THE IMAGE(S) OF THE "CONSUMER IN EU LAW: LEGISLATION, FREE MOVEMENT AND COMPETITION LAW (Dorota Leczykiewicz & Stephen Weatherill ed., Hart Publishing 2016).

[27] See, e.g., Case 48/69, Imperial Chem. Indus. Ltd v. Comm'n, 1972 E.C.R. 619; Case C-557/12, Kone AG v. ÖBB-Infrastruktur AG, ECLI:EU:C:2014:1317, (Jun. 5, 2014).

listing examples like unfair pricing, limiting output, or tying. The concept of "abuse" under Article 102 has evolved through case law, from early formalistic judgments, such as *Hoffmann-La Roche*,[28] to more effects-based approaches exemplified by *Intel*,[29] illustrating the EU's gradual move toward economic analysis.[30] Unlike the AML, EU law contains an exemption regime: agreements that contribute to technical progress or improved distribution may be exempted if they leave consumers a fair share of benefits.[31] This exemption, contained in Article 101(3), demonstrates the EU's attempt to balance competition with innovation and efficiency gains, allowing flexibility where cooperation yields pro-competitive outcomes. EU competition law is animated by economic principles: it aims to promote consumer welfare and market integration, reflecting the EU's long-standing emphasis on market openness and integration.[32] In this sense, competition policy serves as both an economic tool and a constitutional mechanism for European integration, ensuring that market freedoms underpin the broader project of an "ever closer union."

The European Commission (specifically DG Competition, based in Brussels) is the central enforcer. It has exclusive jurisdiction to block mergers of a certain size (under the Merger Regulation 139/2004), and it investigates hard-core cartels and abuse of dominance by undertaking inspections, and can impose fines up to 10% of global turnover.[33] DG Competition operates under a strong investigative mandate grounded in Regulation 1/2003, which decentralised enforcement of Articles 101 and 102 TFEU to Member States while preserving the Commission's primacy in cross-border cases.

National competition authorities (NCAs) in Member States also enforce Articles 101–102 TFEU under the "European Competition Network" model, with the Commission coordinating.[34] Private enforcement (competition damages actions) is far more developed in the EU than in China: any party harmed by anticompetitive conduct can sue in national courts, and EU law

---

[28] Case 85/76, Hoffmann- La Roche & Co. v. Comm'n, 1979 E.C.R. 461.

[29] Case C- 413/14 P, Intel Corp v. Comm'n, ECLI:EU:C:2017:632, (Sept. 6, 2017). (and subsequent GC/ECJ proceedings).

[30] Nicolas Petit, *The Judgment of the EU Court of Justice in Intel and the Rule of Reason in Abuse of Dominance Cases,* 43 Eur. L. Rev. .(2018) 728; Pablo Ibanez Colomo, *The Future of Article 102 TFEU after Intel* (Feb. 17, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125468.

[31] Andreas Scordamaglia- Tousis & Claire- Marie Carrega, *The Application of Article 101(3) in the Context of Multi- Sided Markets Following MasterCard*, Competition Pol'y Int'l (Dec., ,(2014 https://competitionpolicyinternational.com/assets/Uploads/EUDec14-2.pdf>>,.

[32] Konstantinos Stylianou & Marios Iacovides, *The Goals of EU Competition Law: A Comprehensive Empirical Investigation*, 42 LEGAL STUD. 620 (2022).

[33] Council Regulation (EC) No. 139/2004 on the Control of Concentrations between Undertakings (the EU Merger Regulation), 2004 O.J. (L 24) 1.

[34] Council Regulation (EC) No. 1/2003 of 16 December 2002 on the Implementation of the Rules on Competition Laid Down in Articles 81 and 82 of the Treaty, 2002 O.J. (L 24) 1.

provides collective action for cartel victims.[35] Notable EU enforcement examples include heavy fines on global tech firms: for instance, the EU fined Google €2.42 billion in 2017 for favouring its own comparison-shopping service, and €4.34 billion in 2018 for anti-competitive restrictions on Android device makers.[36] EU authorities have similarly pursued Microsoft, Intel, Qualcomm, and other global firms under Article 102.[37] EU competition law thus projects a normative influence: it enforces competition standards beyond borders, and the Commission signs cooperation agreements.[38] The EU's approach emphasises open markets and legal certainty, which differs from China's approach, where regulatory objectives are more closely connected to broader national policy goals.[39]

In the EU, the main actors are the European Commission and national competition authorities. The Commission alone can declare fines and commitments for cross-border cases, though NCAs can act on infringements affecting only a single Member State.[40] The European Court of Justice (ECJ) acts as final arbiter of EU competition law, hearing appeals. The EU model is marked by high institutional independence: Commissioners and DPAs are mandated to act without political direction. This contrasts with China, where enforcement agencies are directly under government.

B. DATA PROTECTION FRAMEWORK

1. China's Data Protection Framework

China's comprehensive data privacy regime is much younger than its competition law. The cornerstone is the Personal Information Protection Law (PIPL) of 2021, which was drafted under the Cyberspace Administration of China (CAC) and came

---

[35] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on Certain Rules Governing Actions for Damages Under National Law for Infringements of the Competition Law Provisions of the Member States and of the European Union, 2014 O.J. (L 349) 1; Sinchit Lai & Zhang Jing, The Tension between Public Interest Litigations and Private Actions under China's Anti- Monopoly Law', 16 Tsinghua China Law Review 19, (2024).

[36] Commission Decision, Case AT.39740 (*Google Search (Shopping)*), June 27, 2017, 2018 O.J. (C 9) 1; Commission Decision, Case AT.40099 (*Google Android*), July 18, 2018 O.J. (C 290) 1.,

[37] Commission Decision, Case COMP/C-3/37.792 (*Microsoft Corp.*), *March 24, 2004, 2007 O.J. (L 32), 23; Commission Decision, Case COMP/C-3/37.990 (Intel Corp.), May 13 2009, 2009 O.J. (C 227) 13;* Commission Decision, Case AT.39740 (*Google Search (Shopping)*), June 27, 2017, 2018 O.J. (C 9) 1; Commission Investigation, Case COMP/AT.40099 (*Facebook / Meta*).

[38] Damien Geradin, Marc Reysen & David Henry, *Extraterritoriality, Comity and Cooperation in EC Competition Law* (SSRN, July 30, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1175003 (accessed Oct. 30, 2025).

[39] Wendy Ng, The Role of Competition Law in Regulating Data in China's Digital Economy, ANTITRUST LAW JOURNAL, 2022, at 841.

[40] Council Regulation (EC) No. 1/2003 of 16 December 2002 on the Implementation of the Rules on Competition Laid Down in Articles 81 and 82 of the Treaty, 2003 O.J. (L 1) 1.

into force on November 1, 2021.[41] The PIPL was designed to protect personal information rights and interests, regulate personal information processing activities, and promote the rational use of personal information.[42] It represents China's first systematic and unified data protection framework, bringing together previously fragmented provisions scattered across cybersecurity and consumer protection laws. It applies to the processing of personal data (defined as information relating to identified or identifiable natural persons) within China and includes an explicit extraterritorial provision similar to the GDPR: it also applies to the processing of Chinese residents' data "outside the borders of the PRC" if it is for the purpose of providing products or services to people in China, or for analysing or evaluating Chinese persons.[43] This extraterritorial clause underscores China's growing assertion of "digital sovereignty," ensuring that foreign companies engaging with Chinese users remain accountable to domestic privacy standards. Importantly, this means that foreign companies processing the data of Chinese nationals may be subject to PIPL if they target the Chinese market.

In terms of substantive requirements, the PIPL establishes principles of legality, fairness, necessity, and good faith, mandating that data processing be based on clear and legitimate purposes. It also introduces GDPR-like concepts such as data minimisation, transparency, and the right of individuals to access, correct, and delete their personal information. It establishes individual rights (access, correction, deletion, data portability in limited cases) and requires separate consent for sensitive personal information (e.g. biometrics, finances). It also mandates security and data localisation measures: for "critical information infrastructure operators" and data exceeding certain thresholds, data must be stored in China and undergo a government security assessment before export. Like the GDPR, the PIPL empowers regulators to order rectification and impose heavy fines for violations. Article 66 provides penalties up to RMB 50 million (or 5% of turnover) for serious breaches, and orders like service suspension. For ordinary violations, fines can reach RMB 1 million. Enforcement is primarily the responsibility of the CAC and its local bureaus (often in coordination with provincial public

[41] Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., August 20, 2021, effective November 1, 2021).

[42] ibid, article 1. Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., August 20, 2021, effective November 1, 2021), art. 1.

[43] Cong Wanshu, *The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics* (SSRN, Feb. 1, 2022), https://ssrn.com/abstract=4019797 (accessed Oct. 30, 2025); Li Wenlong & Chen Jiahong, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR- Inspired Personal Information Protection Law in China* (SSRN, Dec. 13, 2023), https://ssrn.com/abstract=4662817 (accessed Oct. 30, 2025).

security bureaus). For example, in 2023 the CAC fined the China National Knowledge Infrastructure (CNKI) ¥50 million for illegal data collection under PIPL. The PIPL works alongside related laws, notably the Cybersecurity Law (2017) and the Data Security Law (2021), forming China's "three-data" laws framework. Together, they explicitly prioritise national security, public interest, and government control. Unlike the EU, China's law includes provisions allowing cross-border data restrictions or reciprocal measures if other countries impose "discriminatory" limits.[44] It also encourages the State to shape "international rules" for data protection and seek mutual recognition of standards, indicating Beijing's ambition to influence global data governance.[45]

The philosophical underpinning of China's data protection is state‐centric. While the PIPL affirms an individual's personal information rights, under Article 2 PIPL, it frames data protection as being "based on the Constitution" with an eye toward "public interest" and "national security". This framing indicates that privacy protection in China is shaped by legal provisions that balance individual rights with public-interest and security considerations subject to the collective interests of the state and society. In contrast to the liberal rights-based foundations of the GDPR, the PIPL situates individual data rights within the overarching framework of state sovereignty and social order. For instance, Article 10 PIPL prohibits any handling of personal information that harms national security or public interests. The inclusion of "public interest" as a key qualifier grants the state considerable discretion in interpreting compliance obligations, enabling flexible yet politically responsive enforcement. The law requires that government data requests be processed through state authorities under international law principles, and it even empowers reciprocal blocking of foreign data regulations deemed unfair. Hence, China's data law embeds data governance within a broader framework of national regulatory authority and security. Enforcement is administrative and can be swift; the CAC enjoys broad investigatory powers, and works with other agencies (MIIT, police) to audit internet companies. In practice, the Chinese state is deploying these rules to assert cyber-sovereignty: data localisation requirements and censorship of transborder data flows is embedded in a governance system in which central authorities play a substantial role in regulatory oversight. Recent CAC measures, such as the Cross-Border Data Transfer Security Assessment Measures (2022), exemplify this approach by obliging firms to store sensitive data domestically and seek state approval for overseas transfers. The outcome is a system where privacy

---

[44] Li Wenlong & Chen Jiahong, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR‐Inspired Personal Information Protection Law in China* (SSRN, Dec. 13, 2023), https://ssrn.com/abstract=4662817 (accessed Oct. 30, 2025).

[45] *Ibid*, at 44.

regulation functions as both a protective mechanism and an element of China's broader framework for governing digital activity.[46]

2. EU Data Protection (GDPR)

The EU's approach to data protection is rights-based and harmonising. It reflects the EU's broader constitutional vision of protecting individual dignity and autonomy, placing privacy at the heart of European identity. The General Data Protection Regulation (GDPR), Regulation 2016/679, became effective in May 2018 and replaced the older 1995 Directive.[47] Unlike the Directive, which required national transposition, the GDPR is directly applicable across Member States, ensuring full legal uniformity and eliminating fragmentation in national privacy regimes. The GDPR derives from Article 16 TFEU and Charter articles 7 and 8, which establish privacy and data protection as fundamental rights. This dual grounding makes data protection not merely a statutory right but a constitutional guarantee within the EU legal order. It integrates privacy protection with the EU's commitment to human rights, democracy, and rule of law. Its goals are to protect individuals' data in the digital age and to ensure the free flow of personal data within the internal market under a unified regime. The regulation thus seeks to balance two policy aims often in tension: individual rights protection and economic integration through a digital single market.

The GDPR sets out detailed obligations for any "controller" or "processor" of personal data, regardless of nationality. Controllers determine the purposes and means of processing, while processors act on their behalf, creating a layered system of accountability. Organisations must implement technical and organisational measures, conduct data protection impact assessments (DPIAs), and appoint Data Protection Officers (DPOs) where required It defines "personal data" broadly and requires a lawful basis (often consent) for processing. It grants data subjects rights such as access, rectification, erasure ("right to be forgotten"), portability, and the right to object. These rights empower individuals to exercise control over their information and impose significant compliance duties on organisations, enforced by national Data Protection Authorities (DPAs). The GDPR also introduced the principle of "accountability," requiring controllers to demonstrate compliance proactively, rather than

---

[46] Rogier Creemers, Graham Webster, Samm Sacks & *Lorand Laskai, Translation: Outbound Data Transfer Security Assessment Measures-Effective Sept. 1, 2022* (DigiChina, July 8, 2022), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022 (accessed Sep. 7, 2025).

[47] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

merely avoid breaches.

Other lawful grounds include contractual necessity, legal obligation, vital interests, public task, and legitimate interests, each demanding proportionality and transparency in use. Crucially, it is extraterritorial: Article 3 GDPR imposes the regulation on any non-EU organisation processing data of persons in the EU if it offers goods and/or services to them or monitors their behaviour within the EU. This ensures that global digital platforms must comply when targeting EU users.

Enforcement under the GDPR is decentralised. Each Member State has a Data Protection Authority (e.g. France's CNIL, Ireland's DPC) which investigates violations and can issue fines. These DPAs coordinate through the European Data Protection Board (EDPB) to ensure consistency. The GDPR authorises very high fines to deter non-compliance, up to €20 million or 4% of global turnover for serious infringements. The first multi-billion-euro fine under the GDPR was issued in 2023: Meta's Facebook was fined €1.2 billion by the Irish DPC for privacy violations.[48] Many other major fines have been levied: for example, CNIL fined Google €50 million in 2019 for lack of valid consent on personalised ads, and Austria fined Meta nearly €225 million for tracking non-users.[49] In contrast to China, the GDPR emphasizes individual choice, transparency, and market competition rather than explicit state interests. In 2025, the EU advanced a GDPR "Simplification Package" aimed at reducing compliance burdens, particularly for SMEs, by clarifying rules on consent, legitimate interests, international transfers, and enforcement procedures, while reaffirming that the Regulation's core rights-based framework remains intact. This reform initiative reflects an effort to modernise implementation without altering the GDPR's fundamental protections.[50]

III. COMPARATIVE ANALYSIS

---

[48] Irish Data Protection Commission (DPC), *Final Decision in the Inquiry into Meta Platforms Ireland Ltd — Transfers of EU/EEA Personal Data to the U.S.* (May 12, 2023), https://www.edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf.

[49] Commission nationale de l'informatique et des libertés (CNIL), *Restricted Committee imposes a financial penalty of €50 million against Google LLC* (January 21, 2019), https://edpb.europa.eu/news/national-news/2019-cnil-restricted-committee-imposes-financial-penalty-50-million-euros_en (last visited October 30, 2025); Irish Data Protection Commission (DPC), *Final Decision in the Inquiry into Meta Platforms Ireland Ltd — Transfers of EU/EEA Personal Data to the U.S.* (May 12, 2023), https://edpb.europa.eu/news/news/2023-12-billion-euro-fine-facebook-result-edpb-binding-decision_en (last visited October 30, 2025).

[50] European Data Protection Board and European Data Protection Supervisor, *Targeted Modifications of the GDPR: EDPB & EDPS Welcome Simplification of Record-keeping Obligations and Request Further Clarifications* (last visited July 9, 2025), https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_ga.

A. PRINCIPLES AND MODELS OF COMPETITION LAW

The Chinese and EU regimes reflect deeper ideological and institutional differences that extend beyond competition law and data governance. China's AML operates within a regulatory system where the state plays a significant coordinating role in market governance, where competition serves not only as a mechanism for efficiency but also as a tool for achieving national policy objectives, [51] Its stated objectives include enhancing "economic efficiency" and "the interests of society as a whole", implying that competition enforcement can be subordinated to broad social goals.[52] For instance, Article 4 AML authorises the State to set competition rules "compatible with the socialist market economy" for macro-economic regulation. In practice, this means that antitrust policy can be used to address the market conduct of major private-sector firms, restructure markets, or curb the influence of powerful digital conglomerates when they are seen to conflict with public objectives. The Alibaba case illustrated this dual purpose, as enforcement combined traditional antitrust analysis with signals of political oversight and systemic regulation of the digital sector.[53]

The EU's Articles 101–102 TFEU are grounded in principles of market integration and competition, a policy approach that prioritises consumer welfare and market functioning: they protect competition to integration, with no explicit reference to social or political goals. Likewise, Chinese data law balances individual privacy rights with broader public-interest and security considerations, whereas EU law treats data privacy as an individual right necessary for a functioning democracy. In enforcement style, the EU emphasises legal certainty and transparency: Commission decisions typically follow thorough economic analysis and allow parties to defend themselves. Chinese enforcement can be faster and more discretionary, sometimes issuing broad compliance letters (as with Alibaba) without lengthy judicial procedures.

Regulatory models also diverge. The EU relies largely on ex post enforcement of its general rules, albeit now supplemented by ex ante tools.[54] China's AML is similarly ex post, but with a system

---

[51] Wendy Ng, *Changing Global Dynamics and International Competition Law: Considering China's Potential Impact*, 30 EUROPEA JOURNAL OF INTERNATIONAL LAW 1409 (2020).
[52] *Ibid.*
[53] Kenneth Khoo, Sinchit Lai & Chuyue Tian, *The Impact of Antitrust Enforcement on China's Digital Platforms: Evidence from SAMR v Alibaba*, INTERNATIONAL REVIEW OF LAW & ECONOMICS (2024).
[54] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance). Damien Geradin, Marc Reysen and David Henry, *Extraterritoriality, Comity and Cooperation in EC Competition Law* (July 30, 2008), https://ssrn.com/abstract=1175003 accessed 30 October 2025; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 327/1

shaped by overarching administrative and regulatory priorities: enforcement often targets sectors undergoing state-led consolidation (e.g. e-commerce, fintech) and may follow macroprudential campaigns.[55] In data protection, the EU's ex post fines and orders are underpinned by an independent oversight structure (DPAs and EDPB) and by rights enforcement.[56] China's data protection is more ex ante in effect: many PIPL provisions (like categorisation of "important data") have been elaborated through subsequent regulations by CAC, and enforcement tends to focus on compliance with broad national directives.[57] Technologically, the Chinese model explicitly addresses emerging tools: the 2022 AML amendment for the first time bans abuse of market power through "data, algorithms, or platform rules", reflecting a proactive stance.[58] The GDPR also addresses new issues posed by digital economy but generally in an incremental manner.[59]

EU law places strong emphasis on individual rights and procedural safeguards, legal certainty, and competitive market structures, whereas the Chinese law places emphasis on regulatory coordination by central authorities and broader policy objectives. This divergence stems from their foundational philosophies: the EU conceives regulation as a safeguard for personal autonomy within a liberal economy, while China views regulation as an instrument of governance and collective stability. In the EU context, individual rights are conceived as limits on state power; in China, state power is the guarantor of both order and progress, making compliance with public policy objectives an integral part of economic regulation. Despite these differences, both systems see themselves as global regulatory leaders, competing for normative influence in international digital governance. The EU often exports the GDPR (the so-called "Brussels Effect") and its competition rules through trade agreements, adequacy decisions, and multilateral negotiations. European institutions actively promote convergence with EU standards, positioning them as the benchmark for trustworthy digital markets and cross-border data

---

[55] Zhijin Liu & Jingyuan Ma, *Competition Law in China: A Law and Economics Perspective*, 3 CONCURRENCES (2020); Wendy Ng, *Changing Global Dynamics and International Competition Law: Considering China's Potential Impact*, 30 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1409 (2020); Graham Greenleaf, *China's Completed Personal Information Protection Law: Rights Plus Cyber- security,* 172 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, 20–23 (2021).

[56] European Data Protection Board, *Data Protection Authority and You*, https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en (last visited October 30, 2025).

[57] Graham Greenleaf, *China's Completed Personal Information Protection Law: Rights Plus Cyber- security,* 172 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, 20–23 (2021).

[58] Tamar Giladi, Shtub & Michal Gal, *The Competitive Effects of China's Legal Data Regim,* 1 JOURNAL OF COMPETION LAW AND ECONOMICS (2022).

[59] Knut Blind, Crispin Niebel & Christian Rammer, *The Impact of the EU General Data Protection Regulation on Innovation in Firms*, ZEW DISCUSSION (2022).

transfers. By contrast, China is beginning to project its data governance model outward through initiatives such as the Digital Silk Road—a key component of the Belt and Road Initiative that promotes infrastructure, cybersecurity cooperation, and digital standard-setting in partner states.[60] These opposing conceptions of digital order create a form of regulatory competition, with third countries increasingly forced to navigate between the EU's rights-based model and China's governance-oriented one. The outcome is not merely a legal divergence but an ongoing divergence in regulatory approaches that influences global digital governance debates, where both regimes wield significant extraterritorial influence in shaping how the world governs data and competition in the twenty-first century. These principles are illustrated in practice through the major enforcement actions later analysed in this article, including China's Alibaba and Meituan cases and the EU's Google and Meta investigations. These examples show how each jurisdiction operationalises its underlying model, state-coordinated market regulation in China and rights-based market integration in the EU, when regulating dominant digital platforms.

These principles are reflected in high-profile enforcement actions. For example, China's reliance on state-guided market governance can be seen in SAMR's approach to the Alibaba "pick-one-of-two" case, while the EU's rights-based and market-integration model is evident in the Google Search and Android decisions. These examples show how each jurisdiction translates its underlying competition philosophy into concrete interventions in digital markets.

These principles are illustrated in key enforcement actions such as SAMR's Alibaba decision and the European Commission's Google investigations, which show how each jurisdiction translates its underlying model into practice. In China, the Alibaba antitrust case was noted above. The investigation into Alibaba's monopolistic practices marked one of the first major applications of China's updated competition framework and sent a clear signal that even the country's largest tech firms were not beyond scrutiny.[61] The case highlighted the government's growing focus on promoting market order and curbing the influence of powerful digital platforms. In the EU, Google and Meta are key examples illustrating how competition and data protection law intersect in the regulation of large digital platforms. Google has faced multiple antitrust probes over the past decade, reflecting

---

[60] A de Jonge, *Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives,* 3 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY (2024).

[61] Competition Policy International, *China Edition-Antitrust Chronicle* (March, 2022), https://www.competitionpolicyinternational.com/wp-content/uploads/2022/03/ANTITRUST-CHRONICLE-China-Edition-March-2022.pdf (last visited October 30, 2025).
https://www.competitionpolicyinternational.com/wp-content/uploads/2022/03/ANTITRUST-CHRONICLE-China-Edition-March-2022.pdf

ongoing concerns about its dominance in digital markets.[62] Beyond the well-known shopping and Android cases, the European Commission in 2018 launched a detailed investigation into Google's online advertising business, examining whether its practices unfairly favoured its own services and hindered rival platforms. This scrutiny has extended beyond competition to data protection. Google's data processing and consent mechanisms have repeatedly been found in breach of the General Data Protection Regulation (GDPR), leading to substantial penalties. For instance, France's CNIL fined Google €150 million in 2019 for failing to provide clear and accessible information about data use, [63]while a subsequent 2022 decision by the EDPB imposed a further €50 million fine related to location tracking practices.[64] On competition, the EU approved Meta's acquisitions of Instagram and WhatsApp but continues to monitor its market power.[65] These cases highlight how EU regulators apply strict liability and fines to digital platforms 'practices. They also show the EU leveraging extraterritorial jurisdiction: many fines were levied on the Irish subsidiaries of US companies even though the companies are headquartered outside the EU. These principles are illustrated in key enforcement actions such as SAMR's Alibaba decision and the European Commission's Google investigations, which show how each jurisdiction translates its underlying model into practice.

B. COMPARISON OF DATA REGIMES

Although both China's PIPL and the EU's GDPR impose consent requirements and provide data subject rights, they diverge on emphasis and enforcement. At first glance, the two frameworks appear convergent: both restrict the processing of personal data to legitimate purposes, require transparency, and empower individuals through consent and withdrawal mechanisms. Yet the ideological foundations behind these similarities differ sharply.

GDPR is grounded in a rights-based framework that emphasises individual autonomy and data protection: personal data belongs to the person and must be used only for specified lawful purposes, as per Article 5 GDPR. This orientation reflects the EU's constitutional commitment to human dignity and

---

[62] Case AT.39740 – Google Search (Shopping): Commission Decision of 27 June 2017; Case AT.40099 – Google Android: Commission Decision of 18 July 2018 (C(2018) 4761)

[63] Commission nationale de l'informatique et des libertés (CNIL), *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC* (January 21, 2019), https://www.edpb.europa.eu/news/national- news/2019/cnils- restricted- committee- imp oses- financial- penalty- 50- million- euros_en (last visted October 30, 2025).

[64] Irish Data Protection Commission (DPC), *Final Decision in the Inquiry into Meta Platforms Ireland Ltd — Transfers of EU/EEA Personal Data to the U.S.* (May 12, 2023), https://edpb.europa.eu/system/files/2023- 05/final_for_issue_ov_transfers_decision_12- 05 - 23.pdf (last visited October 30, 2025).

[65] European Commission, Acquisition by Facebook, Inc. of the consumer communications services provider WhatsApp Inc, Decision of Oct. 3, 2014, IP/17/1369.

autonomy, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights. It has numerous data subject rights and a broad accountability model, placing the burden of proof on controllers to demonstrate compliance and ensuring strong procedural safeguards through independent oversight bodies. PIPL, while similar in many technical requirements, is framed by national security and public order concerns. For example, PIPL's definition of "sensitive personal information" includes not only race or health, but also location and religious belief, and processing of any personal data must not harm China's "security or dignity". Data localisation under PIPL is mandatory for large-scale and "critical" data, reflecting China's desire to keep data in-country, whereas the GDPR forbids mandatory localisation and instead requires adequate safeguards (or an adequacy finding) for transfers.[66] In the EU system, cross-border data flows are seen as integral to economic integration and innovation, provided privacy rights are preserved; by contrast, in China, such flows are treated as potential security vulnerabilities subject to pre-approval and monitoring.[67] Rather than treating privacy as an individual entitlement, analysts often describe China's regulatory framework as treating data as a resource with strategic significance whose management implicates the stability and security of the state.[68]

Enforcement styles differ as well: GDPR enforcement involves quasi-judicial processes and public sanction by independent authorities, while PIPL enforcement is an administrative process by CAC, with the option to involve procuratorates for criminal issues. This results in different accountability structures, European enforcement features a comparatively strong emphasis on procedural transparency, while China's model places more weight on administrative enforcement and regulatory coordination. Both regimes set out heavy fines and even prison for serious breaches, but China's law explicitly contemplates using data protection to further its governance.[69] Consequently, compliance under PIPL often functions as both a legal and political obligation, aligning corporate behaviour with state-defined digital policy goals. Correspondingly, GDPR exports a rights-and-market model globally, whereas PIPL implements an approach that emphasises national regulatory control and security considerations. Together, they represent two competing paradigms for global data governance, one grounded in individual autonomy, the other in collective security.

C. CROSS-BORDER COOPERATION AND DIVERGENCE

---

[66] Li Wenlong & Chen Jiahong, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China*' COMPUT. L. & SEC. REV., Sep. 2024, 105994.
[67] *Ibid.*
[68] *Ibid.*
[69] *Ibid.*

Enforcement practice further illustrates these divergences: SAMR's actions against firms such as Meituan and Tencent emphasise market order, data control, and industrial policy alignment, whereas the EU's investigations into Meta and Google prioritise consumer choice, transparency, and the integrity of the internal market. Embedding these case studies within the enforcement discussion makes the comparative dynamics more explicit. On the international stage, China and the EU both pursue regulatory coordination but do so from markedly different strategic standpoints. Each sees itself as a norm-setter in global governance, yet their philosophies diverge: the EU promotes market liberalisation and rule convergence, while China emphasises sovereignty, control, and pragmatic cooperation aligned with its national interests.

In competition policy, the EU has long negotiated bilateral and multilateral cooperation agreements with a variety of jurisdictions, including China, the United States, Japan, and South Korea, to ensure information exchange and procedural compatibility.[70] In 2013 the EU Commission signed a Memorandum of Understanding with China's antitrust authorities (NDRC and SAIC) to share information and cooperate on cartel and monopoly investigations. China joined the International Competition Network (ICN) in 2008, aligning on many enforcement procedures.[71] These instruments reflect the EU's broader objective of fostering a level international playing field and preventing regulatory arbitrage in global markets.

A particularly significant milestone occurred in 2013, when the European Commission and China's then separate antitrust authorities — the National Development and Reform Commission (NDRC) and the State Administration for Industry and Commerce (SAIC), signed an MoU establishing a formal basis for dialogue and cooperation on antitrust enforcement.[72] This agreement facilitates information-sharing, staff exchanges, and coordination in cartel and monopoly investigations, marking a step toward alignment between the two jurisdictions' competition regimes. China's active participation in the International Competition Network (ICN), which it joined in 2008, further illustrates its willingness to engage in transnational regulatory cooperation and to align procedural norms with international best practices.[73]

However, divergence remains: for instance, China is not party

---

[70] Rasmus Lema, Axel Berger, Hubert Schmitz & Song Hong, *Competition and Cooperation between Europe and China in the Wind Power Sector*, IDS Working Paper No 377, INST. DEV. STUD. (2012).

[71] *Ibid.*

[72] Memorandum of Understanding on Cooperation in the Field of Anti-Monopoly, Eur. Comm.–Nat'l Dev. & Reform Comm'n & State Admin. for Indus. & Com. (China), Brussels–Beijing, Sep. 20, 2013.

[73] International Competition Network (ICN),About the ICN(2024,) https://internationalcompetitionnetwork.org/about (last visited Nov. 7, 2025).

to OECD competition initiatives and sometimes excludes foreign firms from investigations. In data protection, the EU leads multilateral privacy discussions (APEC Privacy Framework, global adequacy standards), whereas China has championed data sovereignty at the UN and ITU.[74]

In the domain of data protection, the EU similarly acts as a leading promoter of international privacy standards. Through instruments such as the APEC Privacy Framework, the OECD Privacy Guidelines, and the Council of Europe's Convention 108+, the EU has contributed to a global discourse that frames privacy as a fundamental right and supports mechanisms for cross-border data adequacy.[75] China has also championed the principle of "cyber sovereignty" in multilateral fora such as the United Nations and the International Telecommunication Union (ITU), promoting a state-centric approach to global data governance.[76] Unlike the EU, which continues to negotiate data transfer frameworks across Asia (including the proposed Global Data Protection Regulation (Asia) initiative), China has yet to develop a comparable outward-looking or reciprocal data transfer architecture.[77] These developments highlight both convergence in institutional engagement and deep divergence in normative outlook. Whereas the EU seeks to globalise market-based and rights-based regulatory norms, China's international approach reflects an emphasis on regulatory autonomy and state-directed governance frameworks over data and competition policy.

A recent flashpoint in EU–China digital relations is the 2024 European Commission proposal to explore a data adequacy arrangement with China. This initiative reflects Brussels' broader ambition to establish interoperable privacy regimes across major global economies. Yet it immediately sparked significant academic and political debate, as observers questioned whether China's data governance framework could ever be deemed "essentially equivalent" to the EU's rights-based standards under Article 45 of the General Data Protection Regulation (GDPR).[78] Critics argue that China's extensive data localisation mandates, its tight censorship regime, and the subordination of privacy rights to state security imperatives are fundamentally incompatible with the EU's conception of personal data as an expression of individual autonomy and dignity.[79]

---

[74] OECD,*Competition Committee* (2024), https://www.oecd.org/daf/competition/ (last visited Nov. 7, 2025).

[75] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013); APEC, Privacy Framework (2015); Council of Europe, Convention 108+ (2018).

[76] Rogier J.E.H. Creemers,China's Conception of Cyber Sovereignty: Rhetoric and Realization ,in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behaviour, Power, and Diplomacy* (Rowman & Littlefield 2020)

[77] *Ibid.*

[78] *Ibid.*

[79] European Commission, *Data protection: Adequacy decisions — how the EU determines if a non-EU country offers adequate protection* (2025),

The issue is further complicated by regulatory frictions over cross-border data flows. European policymakers have voiced persistent concerns about China's mandatory security assessments for outbound data transfers and the requirement that critical information infrastructure operators store data domestically.[80] These provisions, in the EU's view, distort international trade in digital services and hinder the free flow of information essential to global innovation. Conversely, Chinese regulators contend that unrestricted data exports could undermine national sovereignty and expose sensitive information to foreign surveillance or misuse. This regulatory asymmetry underscores the deep normative divide between the EU's open-market, rights-based digital model and China's sovereign, state-managed approach.[81]

Parallel tensions have emerged in the field of competition enforcement. China's State Administration for Market Regulation (SAMR) has on occasion objected to EU merger reviews or antitrust investigations involving Chinese firms, viewing such actions as extraterritorial assertions of jurisdiction over matters affecting Chinese economic interests.[82] From Beijing's perspective, the EU's increasing willingness to scrutinise global transactions under its competition rules reflects a form of regulatory overreach.[83] In turn, the European Commission has grown more vigilant toward Chinese commercial and technological expansion within the single market. This caution is visible in the security screening of Huawei's telecommunications infrastructure, the data-handling practices of Alibaba Cloud, and the content moderation and privacy policies of TikTok. These high-profile cases illustrate how competition, data protection, and security policy increasingly intersect in the EU's digital governance agenda.

Despite these frictions, both sides publicly affirm a shared commitment to international cooperation on technology regulation. In official statements, EU and Chinese authorities emphasise the need for dialogue, interoperability, and mutual respect for sovereignty in digital governance.[84] Notably, China's Personal Information Protection Law (PIPL) includes a clause

---

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/5B99-AM83] (last visited Nov. 7, 2025).

[80] China Briefing Team, *The PRC Personal Information Protection Law (Final): A Full* Translation, China Briefing(Aug. 24, 2021), https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/[https://perma.cc/QJB2-KBW9](last visited Nov. 7, 2025).

[81]Chi Zhang, *China's privacy protection strategy and its geopolitical implications, 3 ASIAN REV. POL. ECON., 2024, at 6.*

[82]Vellah Kedogo Kigwiru, *The European Union's Jurisdiction in Merger Regulation,* SSRN(2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3534986.

[83]Kawsar Uddin Mahmud, *China-EU Trade Conflict: Implications for the Global* Economy,Modern Diplomacy (Jan.29,2025), https://moderndiplomacy.eu/2025/01/10/china-eu-trade-conflict-implications-for-the-global-economy/ (last visited Nov.7 2025).

[84]Hunter Dorwart, *Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts,*in HIDEYUKI MATSUMI, DARA HALLINAN, DIANA DIMITROVA, ELENI KOSTA & PAUL DE HERT (eds.), Data Protection And Privacy, Volume 15: In Transitional Times (Hart Publishing, 2023).

encouraging the joint formulation of international norms on personal information protection, suggesting Beijing's desire to position itself as an active participant in global rule-making.[85]

In practice, however, the scope for substantive convergence remains limited. While the EU continues to anchor its digital policy in individual rights, transparency, and market fairness,[86] China prioritises collective interests, state security, and multilateral, state-led governance mechanisms.[87] This enduring divergence arises from underlying differences in institutional design and regulatory priorities: the EU's liberal constitutionalism versus China's developmental and statist governance model. The evolving dialogue on data and competition thus encapsulates a broader struggle over the future architecture of global digital order, one that pits normative universalism against digital sovereignty. A high-profile Chinese case is Tencent's recent antitrust settlement regarding its exclusive contracts for streaming rights, which similarly involved abuse of dominance and the ending of such practices.[88] The settlement followed concerns that Tencent's exclusive deals restricted market entry for competitors and limited consumer choice, prompting regulators to intervene and require fairer licensing terms. This case, like Alibaba's, showed how Chinese authorities are extending antitrust oversight into different corners of the digital economy, including media and entertainment. Both illustrate China's efforts to break up platform exclusivity across e-commerce, gaming, and media, creating a more competitive environment that aligns with national regulatory goals.

On the data side, Chinese authorities have targeted domestic companies for PIPL violations. Enforcement has become more frequent and visible, reflecting a stronger emphasis on compliance and the protection of citizens' personal information. For example, ride-hailing giant Didi was forced to delist after the Cyberspace Administration of China (CAC) cited data security risks and inadequate handling of sensitive user data. This case drew international attention and underscored how data regulation is now tightly linked to questions of national security. Similarly, various apps have been fined or suspended for illegal data collection practices, illustrating that smaller companies, too, face increasing scrutiny. For instance, smartphone maker Xiaomi came

---

[85]Hugh Roberts, Emily Hine & Luciano Floridi, *Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance,* in MARINA TIMOTEO, QUO VADIS, SOVEREIGNTY?: NEW CONCEPTUAL AND REGULATORY BOUNDARIES IN THE AGE OF DIGITAL CHINA 123 (PHILOSOPHICAL STUDIES SERIES, SPRINGER 2023), (Barbara Verri & Riccardo Nanni eds.).

[86]Mateusz Grochowski, Agnieszka Jabłonowska, Francesca Lagioia & Giovanni Sartor, *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises,* 8 CRITICAL ANALYSIS OF LAW 43 (2021).

[87]Alice De Jonge, *Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives,* 32 INT'L J.L. & INFO. TECH. (2024).

[88]*Ibid.*

under investigation in 2022 for issues related to excessive data access permissions and unclear user consent procedures.[89] These enforcement actions show SAMR and CAC using their new powers to rein in tech giants and reinforce accountability in the digital sector. They also demonstrate a broader policy objective: to balance innovation and growth with state control, user protection, and social stability.

Comparatively, Chinese tech firms are chiefly subject to Chinese law, whereas international companies must navigate both regimes. For example, TikTok (ByteDance) was recently subject to U.S. and EU data inquiries, while also being closely regulated under Chinese cybersecurity norms for its global business.[90] Similarly, Alibaba's international cloud and fintech arms have had to consider GDPR compliance in Europe alongside PIPL compliance in China.[91] The overlapping jurisdictions can lead to conflicts: the EU sometimes accuses China of extraterritorial data laws that breach fundamental rights, while Chinese authorities view EU privacy and competition rules as unfair constraints on Chinese firms.[92] Nonetheless, there are instances of dialogue: Google has made voluntary commitments in China (e.g. restricting certain services), and Alibaba Group reportedly complied with CAC's data security reviews for its local fintech arm.[93]

Tech firms have become the testing ground for these regimes: how Chinese and EU regulators treat e-commerce, social media, and platform services reveals their different priorities, competition and consumer welfare in the EU, versus industrial order and security in China.[94] A prominent illustration on the EU side is the series of enforcement actions involving Meta (Facebook), which encapsulate the Union's rights-based, consumer-centred, and transparency-driven regulatory model. Meta has consistently been scrutinised for practices that restrict user autonomy or distort competitive conditions, reflecting the EU's view that data governance and market power are deeply interconnected. A defining example occurred in 2023, when the

---

[89] *Ibid.;* Cyberspace Administration Of China, *Penalty Decision on Didi Chuxing Technology Co.,* Ltd.(July 21, 2022)*;* DAN WEI, *China's Data Governance: Between* Development and Protection(2023), https://ssrn.com/abstract=4542981 accessed(last visited Oct.30, 2025).

[90] Seedata Protection Commission, *Inquiry into TikTok Technology Limited – April 2025(IN2192)* (Apr. 30, 2025), https://www.dataprotection.ie/en/treoir- ccs/law/decisions/inquiry- tiktok- technology- limited- april- 2025(last visited .October 30, 2025).

[91] Alibaba Cloud, GDPR Compliance Highlights, https://www.alibabacloud.com/trust-center/gdpr (last visited Oct.30,2025).

[92] Sangwoo Lee, *A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing(2018),* https://ssrn.com/abstract=3442428(last visited Oct.30,2025).

[93] *Ibid.*

[94] Kena Zheng & Francis Snyder, *China and EU's Wisdom in Choosing Competition Soft Law or Hard Law in the Digital Era: A Perfect Match?,* 9 CHINA-EU L.J. 25 (2023).

Irish Data Protection Commission fined Meta €1.2 billion for unlawful transfers of EU user data to the United States.[95] Although formally grounded in data-protection law, the decision had significant competitive implications: it directly constrained the company's ability to leverage cross-border data flows across its integrated services, thereby limiting the structural advantages of its scale and data concentration. EU authorities have also challenged Meta's reliance on personalised advertising based on "contractual necessity," finding that users were not offered a genuine choice regarding behavioural-tracking practices. These findings align with the EU's commitment to ensuring informed consent, market transparency, and fair competition within the internal market.

Together, these enforcement actions demonstrate how the EU deploys legal tools, spanning both competition and data-protection domains, to discipline digital gatekeepers, curb exploitative data practices, and preserve user rights. In contrast to China's policy-aligned and state-centred enforcement model, the EU's approach emphasises accountability, procedural oversight, and the protection of individual autonomy as integral components of market regulation.

D. EXTRATERRITORIALITY AND GLOBAL INFLUENCE

Both jurisdictions extend their reach beyond their borders. The AML expressly applies to foreign companies whose conduct has anticompetitive effects in China.[96] Chinese merger control likewise reviews foreign-to-foreign deals if they meet Chinese thresholds.[97] China thus asserts extraterritorial jurisdiction when Chinese market interests are at stake. The PIPL does similarly for personal data of Chinese citizens processed abroad. These provisions allow China to regulate the global operations of companies like Alibaba, Tencent, and even foreign firms like Microsoft or Amazon if they impact China.

The EU's extraterritoriality is likewise significant. Article 3 GDPR covers foreign processors targeting EU persons, so it applies to, say, U.S. tech companies handling EU user data. In competition, the EU has a "effects doctrine": under Regulation 1/2003 the Commission can investigate conduct with substantial anti-competitive effects on the EU market, even if the firms are foreign. Additionally, EU merger rules apply to cross-border mergers affecting EU commerce. Thus, European law can

---

[95]European Data Protection Board, EDPB Binding Decision 13 April 2023 — Administrative fine against Meta Platforms Ireland Ltd.'(Data *Prot. Comm'n*Commission, May *22,*2023,)https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (last visited Dec.7,2025).

[96]Emanuela Lecchi*, Hong Kong, China, and the Disruption of Antitrust,31 WASH. INT'L L.J. (2022).*

[97] International Chamber of Commerce, *ICC Merger Control Recommendations* (2024), https://icc.se/wp-content/uploads/2025/02/2024_ICC-Merger-Control-Recommendations.pdf, (accessed Oct.30, 2025).

influence corporate behaviour worldwide. This is part of the so-called "Brussels effect," whereby the EU's high standards effectively shape global norms.[98] For example, many multinational companies pre-emptively adopt GDPR-style privacy policies worldwide.

China's international legal influence is now rising. Scholars have dubbed this the "Beijing Effect," noting that Chinese standards (in data governance, surveillance, e-commerce regulation) are being exported along Belt and Road projects and through compliance demands by Chinese firms abroad.[99] China is also active in international standard-setting bodies (ISO/IEC on privacy, UN discussions on digital trade).[100] However, China's influence is the subject of differing interpretations among observers: some countries resist China's model of cybersecurity restrictions. The PIPL's provisions on international cooperation and reciprocity indicate that China intends to play a rule-making role, but its emphasis on state sovereignty often clashes with EU and U.S. calls for open data flows.[101]

In international fora, China and the EU sometimes find common ground—both, for example, support anti-cartel initiatives at the WTO and emphasize the importance of fair competition in global trade. However, they often diverge sharply on digital governance. The EU continues to promote human-rights-oriented norms, exemplified by its sponsorship of UN resolutions on privacy and data protection, whereas China favours a sovereignty-based, state-led model of internet governance grounded in national security and collective welfare. Cooperation in competition policy remains largely pragmatic: while memoranda of understanding (MOUs) between the European Commission's DG COMP and China's State Administration for Market Regulation (SAMR) have facilitated dialogue and technical exchanges, geopolitical tensions, especially trade disputes and technological rivalry, frequently strain enforcement coordination. In recent years, Chinese officials have voiced frustration when EU agencies investigate Chinese firms on competition grounds, perceiving such actions as politically motivated. Conversely, the EU has criticised China's antitrust system for opacity, limited judicial transparency, and the perceived prioritisation of industrial policy over procedural fairness. Despite these tensions, both jurisdictions remain

---

[98] Anu Bradford, *The Brussels Effect,* NORTHWESTERN UNIVERSITY LAW REVIEW VOL 107 NO.1, Dec. 1, 2012, at 1.

[99] Matthew S. Erie&Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 NYU JOURNAL OF INTERNATIONAL LAW & POLITICS, 2021, at 1.

[100] Junhua Zhu, Elina Sinkkonen and Mikael Mattlin, *Strategic Technology Competition Revisited: The Co-Evolution of China's National Innovation System and Artificial Intelligence Standardisation Strategy*, (Nov. 26, 2025), https://ssrn.com/abstract=5277549.

[101] Igor Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, SMART CITIES 5(3), Sep. 8, 2022, at 1129.

influential actors in the evolving global regulatory landscape. Their distinct approaches contribute to a broader patchwork of international law, where regional norms compete and converge. The EU's GDPR and competition rulings have turned it into a "norm entrepreneur," while China's rapid digital regulation provides both inspiration and caution for emerging markets seeking to balance innovation with control.

Empirical evidence reinforces both the Brussels Effect and the emerging Beijing Effect. The Brussels Effect is well documented: Bradford's foundational study shows how the GDPR's extraterritorial scope has prompted countries such as Brazil (LGPD), Japan (APPI reforms), South Korea (PIPA amendments), and Kenya to adopt EU-style data-protection regimes, while multinational firms increasingly internalise EU standards globally to avoid regulatory fragmentation.[102] Subsequent empirical work confirms that the GDPR's Article 3 has forced U.S. technology firms, including Meta, Google, and Amazon, to restructure data-processing operations worldwide, demonstrating how EU rules shape corporate behaviour beyond EU borders.[103] The EU's adequacy regime also drives convergence, as third countries routinely revise privacy legislation to obtain adequacy status—most recently South Korea, Japan, and the UK—illustrating a measurable regulatory pull. By contrast, the Beijing Effect operates through infrastructure, investment, and technical standard-setting rather than market size alone. Erie and Streinz's fieldwork on China's Digital Silk Road shows how Chinese data-governance norms, especially data-localisation, cybersecurity review, and digital infrastructures that incorporate security and monitoring functionalities as part of their technical design, are exported through digital infrastructure projects in Central Asia, Africa, and Southeast Asia.[104] Similarly, Chinese outbound tech firms, including Huawei, Alibaba Cloud, and ZTE, disseminate Chinese technical standards through turnkey digital-governance systems, often requiring host states to adopt Chinese-style security protocols as part of contractual arrangements.[105] Empirical studies of African and Asian DSR partners demonstrate the uptake of Chinese cyber-sovereignty principles, particularly in Ethiopia, Pakistan, and Laos, where national data and cybersecurity laws mirror elements of China's regulatory logic.[106] In this respect, these developments show that

---

[102] Anu Bradford, *supra* note 98, at 1.

[103] Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID, 145 Laws Show GDPR Dominance?* (UNSW Law Research Paper No 21-44, 2021).

[104] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems,* GERMAN LAW JOURNAL, 2017, at 881.

[105] Rogier Creemers, *China's Social Credit System and Public Governance: A Comprehensive Introduction* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 (accessed Dec.7, 2025).

[106]Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, *in* GOVERNING CYBERSPACE: BEHAVIOUR, POWER, AND DIPLOMACY, 107–142 (Dennis

both the EU and China exert global regulatory influence, one through market-driven legal convergence, the other through infrastructural and geopolitical diffusion.

IV. CONCLUSION

The comparison between China and the European Union demonstrates that their regimes in competition law and data protection have evolved into highly developed systems that nevertheless rest on fundamentally different normative and institutional foundations. China's Anti-Monopoly Law and the Personal Information Protection Law operate within a regulatory architecture that assigns state institutions a prominent role in coordinating markets and data governance. The Chinese framework consistently links competitive ordering with national development goals, industrial upgrading, and social stability. Similarly, the PIPL reflects a model in which personal data governance is closely connected to national security and economic sovereignty. Together, these fields of law express a regulatory philosophy that regulates markets and data flows in ways that reflect broader national policy objectives. Individual rights and market autonomy are protected, but they are situated within a wider collective and security-oriented context.

The European Union's legal order embodies a markedly different orientation. Its competition law regime is grounded in the principles of the internal market, economic liberalisation, and institutional independence. Enforcement mechanisms are designed to preserve undistorted competition and safeguard consumer welfare. In the field of data protection, the EU relies on a rights-based constitutional model that treats privacy and data protection as fundamental rights embedded in the Treaty and the Charter. The GDPR illustrates how the EU integrates economic regulation with a strong commitment to individual autonomy and democratic values. The result is a system in which the market is regulated to protect consumers and ensure openness, and in which personal data governance is centred on rights, transparency, and proportionality.

While these differences are significant, the analysis also reveals selected areas of convergence that reflect the shared challenges posed by digitalisation. Both jurisdictions are increasingly attentive to the growing influence of large technology platforms and recognise the need to regulate digital ecosystems. Both claim extraterritorial effects where domestic markets or data subjects are implicated, which reflects a broader global trend toward assertive regulatory jurisdictions. Furthermore, both China and the EU influence international debates, whether through the EU's projection of rights-based norms or China's promotion of cyber sovereignty and data security principles. The case studies

---

Broeders & Bibi van den Berg eds, 2020).

considered in the article show that although their enforcement philosophies diverge, each jurisdiction applies its core principles consistently when responding to similar forms of digital market power.

The comparison highlights that China and the EU represent two influential yet distinct models of digital governance, each grounded in its own constitutional, political, and economic traditions. Understanding their competing orientations is essential for interpreting how global regulatory dynamics are likely to evolve as digital markets expand. Whether the future international landscape will reflect continuing divergence, selective alignment, or a form of pragmatic coexistence will depend on how each system adapts to technological change and how global actors navigate the coexistence of these two regulatory paradigms.