COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

CENTRAL BANK DIGITAL CURRENCIES AND PRIVACY: A COMPARATIVE ANALYSIS OF REGULATORY APPROACHES IN THE EU AND CHINA

Sonia Sforza

TABLE OF CONTENTS:

Central bank digital currencies (CBDCs) raise complex challenges concerning privacy, as they operate at the intersection of individual data protection, public interest, and state oversight.
This paper aims to propose a comparative assessment of the governance frameworks underpinning the digital euro and the e-CNY, the CBDCs respectively developed by the European Union and the People's Republic of China. This study focuses on how privacy is conceptualized and regulated in each model, taking into account their distinct legal traditions, specific sociocultural context and societal priorities.
The comparative analysis carried out in this paper also serves to reflect on the potential global implications of the two models, in a field where the development of common standards is essential to enable cross-border payments and, more broadly, to ensure the successful implementation of CBDCs.

Keywords: Central Bank Digital Currency; privacy; personal data protection; surveillance; European Law; Chinese Law; Brussels Effect; Beijing Effect

I. INTRODUCTION

The progressive digitalisation of monetary systems has brought Central Bank Digital Currencies (CBDCs)[1] to the forefront of both institutional and academic debate[2].

[1] Although there is no internationally agreed definition, certain recurring characteristics emerge in regulatory practices of CBDCs. These include: the classification of a CBDC as legal tender; its nature as a direct liability of the issuing central bank (see T. Mancini-Griffoli *et al.*, *Casting Light on Central Bank Digital Currency*, IMF Staff Discussion Note (2018), at 6); the possibility of issuance and distribution through centralised technological infrastructures or, subordinately, hybrid or partially decentralised infrastructures (see BIS, *Central bank digital currencies: foundational principles and core features*, Report n. 1 (2020), at 15). Additionally, if the CBDC is accessible to end users (households and businesses), it is referred to as a retail CBDC; if the CBDC is only available to certain institutions, mainly banks, it is referred to as a wholesale CBDC. See J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, Seton Hall L. Rev., 54 (2023), at 71.

[2] Globally, interest in these instruments is reflected in a wide array of projects, involving over 134 countries and monetary unions. See Atlantic Council, *Central Bank Digital Currency Tracker*, available at https://www.atlanticcouncil.org/cbdctracker/ (last visited Jul. 23, 2025). To date, three jurisdictions have launched a CBDC: the Bahamas, Jamaica and Nigeria. The Chinese digital yuan is currently the largest CBDC pilot project in the world, with a transaction volume of $986 billion in June 2024. Among the motivations for developing CBDCs, it is possible to identify a tendency among developed countries to regard their issuance as a means of safeguarding monetary sovereignty in the face of increasing competition from the private sector within the payments market, a competition most notably embodied by crypto-assets and, in particular, by stablecoins (see L. Beltrametti, G. B. Pittaluga, *Monetary Policy Implications of Stablecoins and CBDCs*, Economia internazionale, 76 (III, 2023), at 468-469, who highlighted widespread concern about stablecoins as a tool that could potentially undermine the monetary sovereignty of central banks, with negative consequences for the overall stability of the financial system). Conversely, in developing countries, the adoption of CBDCs appears primarily (though not exclusively) to aim at fostering financial inclusion by

Conceived as digital forms of legal tender issued by central banks, CBDCs differ from cash not only in their technological infrastructure, but also in the quantity and granularity of data they may generate through each transaction. Among the various legal and policy issues raised by these instruments, one of the most paradigmatic is the potential for central banks to collect massive amounts of data on end users. Such data aggregation raises serious concerns regarding mass surveillance, increases cybersecurity vulnerabilities, and opens the door to potential abuse or misuse by state authorities, particularly in the absence of clear and stringent safeguards[3]. These risks are further compounded by the involvement of private intermediaries, whose participation in the CBDC ecosystem can generate additional layers of data processing, thereby amplifying the potential for both security breaches and improper use of sensitive information[4].

This article aims to investigate – from a comparative perspective[5] and taking into consideration ideological, institutional, and socio-cultural foundations – how two major global actors, the European Union and the People's Republic of China[6], have approached the issue of privacy protection in the design and regulation of their respective CBDCs: the digital euro and the digital yuan (or e-CNY). The objective of this study is to understand how the regulators of both systems address, concretely, the delicate balance between control, efficiency, and individual freedom, thereby revealing whether, and to what extent, the legal system prioritizes the protection of the individual, collective security, or the safeguarding of institutions.

The analysis of the regulatory choices concretely adopted by these jurisdictions fits within the broader and growing body of legal scholarship on privacy and CBDCs. However, while the doctrinal debate has largely focused on theoretical aspects of the issue – such as CBDC design models that enhance privacy and the necessary balancing between privacy rights

expanding access to safe and efficient payment services for unbanked population (see: IMF, *Central Bank Digital Currency's Role in Promoting Financial Inclusion* (2023), at 2; A. Kosse, I. Mattei, *Making headway-results of the 2022 BIS survey on central bank digital currencies and crypto*, BIS Papers (2023), at 7).

[3] J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 112.

[4] *Id.*, at 113.

[5] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati (5th ed. 2024); R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)*, The American Journal of Comparative Law 39 (I, 1991); M. Cappelletti, The Judicial Process in Comparative Perspective (1989).

[6] The decision not to include the United States in the core comparative analysis of this article is a conscious and methodologically motivated choice, grounded in the specific and distinctive approach adopted by U.S. authorities towards CBDCs. In contrast to jurisdictions actively developing retail CBDCs, the United States has recently taken a markedly different stance. In 2025, a presidential executive order formally prohibited the establishment, issuance, and circulation of a CBDC at the federal level (Executive Order of the President of the United States, *Strengthening American Leadership in Digital Financial Technology*, 23 January 2025, available at https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/). This decision reflects long-standing concerns within the U.S. debate regarding the potential implications of CBDCs for individual privacy, the distribution of monetary power, and the role of the state in financial intermediation. Opponents of a U.S. CBDC have argued that the introduction of a digital dollar could facilitate excessive governmental control over financial transactions and pose risks to civil liberties, while also disrupting the existing two-tier banking system. In this context, policy discourse has increasingly favoured market-based alternatives, particularly privately issued, dollar-denominated stablecoins, as instruments capable of supporting payment innovation without expanding the role of the central bank in retail finance (see D. Krause, *The Implications of a U.S. Ban on Central Bank Digital Currencies: Global Financial Dynamics and the Future of Payments* (2025), at 5-6).

and anti-money laundering/counter-terrorism financing objectives[7] – relatively little attention has been paid to the specific regulatory solutions adopted by individual jurisdictions[8].

In this still-evolving field, the comparative analysis assumes a fundamental role, as it enables the examination of heterogeneous regulatory models, the identification of convergent or divergent regulatory approaches, and critical reflection on the prospects for legal harmonisation or normative circulation.

This need is not merely theoretical, but also finds practical resonance in the increasing international focus on the potential for cross-border payments through CBDCs[9]. In this context, the concept of interoperability between different CBDCs acquires central importance. This term refers to the technical and operational capacity of digital currency systems issued by distinct monetary authorities to interact with one another, that is, to ensure mutual recognition and immediate convertibility[10]. In a globalised economy, achieving this objective appears to be of strategic importance in order to ensure the efficiency of cross-border transactions, reduce transaction costs, and promote financial inclusion[11]. However, technical interoperability necessarily presupposes a certain degree of legal interoperability[12]. The ability of different CBDCs to interact cannot disregard the existence of a lowest common denominator in relation to certain fundamental regulatory choices, particularly those concerning user identification, data ownership, as well as the allocation of access and control powers between public and private entities[13]. The absence

[7] K. P Murphy *et al.*, *Central Bank Digital Currency Data Use and Privacy Protection*, IMF – Fintech Notes (2024); Z. Wang, *Money laundering and the privacy design of central bank digital currency*, Review of Economic Dynamics, 51 (2023); N. Pocher, A. Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, IEEE transactions on network and service management, 19 (II, 2022); J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit..

[8] G. Kaur, *Privacy implications of central bank digital currencies (CBDCs): a systematic review of literature*. EDPACS, 69 (IX, 2024). The author conducted a literature review on the topic of CBDCs and privacy, identifying the areas that have attracted the most scholarly attention as well as the existing gaps. He highlighted that the approaches to privacy in CBDC design vary significantly across jurisdictions; however, few comparative assessments have been conducted, and in many cases, national privacy strategies remain opaque. Therefore, further comparative research could help clarify these divergences, contributing to the development of comprehensive legislative frameworks.

[9] Traditional cross-border payments are money transfers between parties located in different jurisdictions. These payments have been criticised for their high costs, slow execution, limited access and lack of transparency. Due to these critical issues, the G20 has identified the improvement of cross-border payments as a global priority. In this context, CBDCs represent an opportunity to rethink existing payment infrastructures, overcoming many of the current inefficiencies thanks to the possibility of designing shared solutions from the outset. However, this potential can only be realised if central banks consider the international dimension in the design of their digital currencies from the outset and coordinate to ensure interoperability. CPMI, BIS Innovation Hub, IMF and World Bank, *Options for access to and interoperability of CBDCs for cross-border payments*, Report to the G20 (2022), at 1-3.

[10] *Id.*, at 5.

[11] For example, CBDCs could be used by immigrant workers to send money to their families without the traditional transaction costs. See J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 87.

[12] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs* (2024), at 25; C. Mu, *Theories and practice of exploring China's e-CNY, Data, Digitalization, Decentralized Finance and Central Bank Digital Currencies: The Future of Banking and Money* (2023), at 187.

[13] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 25.

of a shared regulatory framework in these areas ultimately risks undermining not only user trust but also the overall success of CBDCs themselves[14].

Ultimately, building on these insights, this paper will analyse the potential influence that both the EU and PRC may exert on international regulatory trends, especially in a field that is devoid of common standards but where common standards are needed. On one side, the European Union has already demonstrated the capacity to shape foreign legal systems through the so-called Brussels Effect[15]. On the other, PRC may exert influence by leveraging its geopolitical network through the Belt and Road Initiative (BRI). In this light, the governance models of CBDCs adopted by these two actors may contribute to shaping future global standards in the field of CBDCs, particularly as regards privacy and data governance.

II. CBDCs and Privacy Protection: A Theoretical Framework

Before proceeding, it is necessary to provide a theoretical premise regarding the specific relationship between CBDCs and the protection of personal data. The implementation of CBDCs is expected to lead to an exponential increase in the volume of financial data in circulation, data that is particularly sensitive, as it can reveal numerous personal characteristics, and which may therefore significantly affect individual freedom[16].

The issue outlined above arises from the fact that a CBDC, as mentioned, does not merely represent the dematerialised transposition of physical cash[17]. Rather, it entails regulatory choices that embody a structural tension between the protection of privacy and the safeguarding of public interests.

---

[14] CPMI, BIS Innovation Hub, IMF and World Bank, *Options for access to and interoperability of CBDCs for cross-border payments*, cit., at 3; C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, in N. Bilotta, F. Botti, The (Near) Future of Central Bank Digital Currencies. Risks and Opportunities for the Global Economy and Society (2021), at 186.

Indeed, in a hypothetical scenario in which interoperability between CBDCs does not materialise, the risk emerges that digital currencies may reproduce, rather than overcome, the structural fragmentation of the current international payment system. In such a context, different regions could progressively align with distinct monetary and technological blocks, depending on economic ties, geopolitical influence, or infrastructural dependence. The absence of interoperability would thus limit the effectiveness of CBDCs in facilitating cross-border transactions and could result in the duplication of existing correspondent banking arrangements, along with their associated costs, delays, and barriers to access. Rather than constituting a transformative innovation, CBDCs would risk becoming digital replicas of the traditional system, thereby undermining their capacity to enhance efficiency, inclusion, and transparency in international payments. At the same time, even in the absence of full interoperability, forms of partial or functional interoperability could emerge, for instance through bilateral or multilateral arrangements, shared technical standards, or interoperability layers designed to enable limited cross-border use without full regulatory convergence. Such solutions, however, would likely remain fragile, as they would operate against the backdrop of divergent legal frameworks, particularly with respect to data governance, user identification, and the allocation of control between public and private actors. Against this background, the absence of interoperability would not merely represent a missed opportunity, but could actively undermine the transformative potential of CBDCs in the cross-border context.

[15] A. Bradford, The Brussels Effect: How the European Union Rules the World (2020).

[16] A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk* (2024), at 8.

[17] Unlike any other digital payment method, cash is still the most privacy-friendly form of payment, as it is the only tool that guarantees complete anonymity. See: C. M. Khan *et al.*, *Money is Privacy*, Int'l Econ. Rev., 46 (II, 2005), at 377.

In this regard, it is no coincidence that the international debate has raised concerns about the potential use of CBDCs by authoritarian regimes for purposes of surveillance and political repression, with the attendant risk that the comprehensive monitoring of individual transactions may be exploited not for strictly economic objectives, but for political and social control[18]. Indeed, the architecture of many CBDC systems allows central banks – and, through them, state authorities – direct and real-time access to users' transactional data, thereby opening up ambivalent scenarios. On the one hand, this capability provides an important tool for monitoring financial flows, preventing criminal activities, and improving the overall efficiency of the monetary system[19]. On the other hand, such access could be used to restrict political action, for instance through the selective blocking of payments or the economic exclusion of individuals deemed "undesirable"[20].

In light of these risks, it is evident that design choices concerning CBDCs are never neutral: the way in which a digital currency is structured directly influences the degree of privacy protection and the safeguarding of fundamental rights[21]. In this context, the principle of privacy-by-design, whereby the protection of privacy must be embedded from the earliest stages of system development, assumes a pivotal role[22]. It is the responsibility of regulators to define the fundamental rights that must be effectively guaranteed and integrated into technological infrastructures, as well as to set clear limits on data control by the various actors involved[23]. A regulatory approach lacking in specific guidance – or, worse, entirely absent – risks legitimising the creation of opaque systems in which the rights and obligations of the parties involved are difficult to identify.

From this perspective, regulatory choices (or the absence thereof) and the consequent design of CBDCs ultimately constitute a political matter, as they presuppose a decision

---

18 K. Takami, *China's Bid for Digital-Yuan Sphere Raises Red flags at G-7* (2021), available at https://asia.nikkei.com/Spotlight/Cryptocurrencies/China-s-bid-for-digital-yuan-sphere-raises-red-flags-at-G-7 (last visited Jul. 23, 2025); R. Khalaf, H. Warrell, *UK spy chief raises fears over China's digital renminbi* (2021), available at https://www.ft.com/content/128d7139-15d6-4f4d-a247-fc9228a53ebd (last visited Jul. 23, 2025).

19 C.-Y. Tsang *et al.*, *Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence*, Nw. J. Int'l L. & Bus., 43 (2023), at 258.

20 N. Rancie *et al.*, *Central Bank Digital Currency (CBDC) and Digital Euro*, Economic and Social Development: Book of Proceedings (2024), at 4. Consider, for example, contexts in which political opposition is considered an illegal activity, making financial tracking a tool for political control. See M. Warren, *Let the Digital Euro Circulate: Introducing a Retail C.B.D.C. in the Eurozone with Unlimited Holdings by Users*, University of Bologna Law Review, 8 (I, 2023), at 20).

21 For an analysis of the various design choices, see J. Mascelli (2023). *Data Privacy for Digital Asset Systems*, Finance and Economics Discussion Series, Washington: Board of Governors of the Federal Reserve System, 59 (2023).

22 See N. Pocher, A. Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, cit.. The principle of privacy-by-design falls within the broader scope of regulation-by-design, constituting a specific application of the latter to the protection of personal data. Regulation-by-design is an approach that aims to incorporate regulatory requirements directly into the technical design of systems, creating tools that are inherently compliant with the rules. This approach evolved from Lessing's concept of "code is law", according to which behaviour in cyberspace must be controlled by software code. See L. Lessig, Code v. 2.0. (2006). The principle of privacy-by-design is a cornerstone of data protection: it was already highlighted in a UN recommendation (Report of the Secretary-General, UN doc. A/74/821) and has also been adopted in the GDPR (Art. 25 and Recital 78).

23 K. Rommetveit *et al.*, *Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering*, Privacy and Identity Management: The Smart Revolution, 526 (2018), at 32.

regarding the level of privacy to be afforded to users and the degree of access to their data permitted to public and private actors[24].

The tension between public control and the protection of fundamental rights becomes even more pronounced in the international context, particularly insofar as CBDCs may be used to facilitate cross-border payments[25]. In such scenarios, the issuing central bank could potentially obtain access to the personal data of individuals residing in other jurisdictions. The establishment of common standards regarding privacy and data governance in relation to CBDCs therefore becomes, as already noted, essential to prevent regulatory asymmetries.

These theoretical considerations form the necessary starting point for the analysis of the regulatory and technical solutions adopted in the principal reference models, particularly when examined in light of their specific institutional, social, and cultural contexts.

III. Privacy Protection in the European Union: An overview

The European Union's longstanding commitment to balancing technological innovation with the protection of fundamental rights and European values constitutes a cornerstone of its digital strategy[26]. In fact, in its process of digital transformation, the EU pursues a model that may be defined as human-centric, aimed at reconciling technological innovation with the safeguarding of fundamental rights. This is reflected in the EU's intention to build an inclusive digital ecosystem, where citizens and businesses can operate and thrive under fair conditions. According to this vision, digital infrastructure must remain an open and democratic space, where technologies serve society as tools at its disposal[27].

Moreover, as digitalisation progressively permeates all societal spheres, the protection of personal data has, over the years, assumed an increasingly central role.

The European journey in the field of privacy began with Directive 95/46/EC[28], which for the first time provided a harmonised framework for the protection of personal data within the EU. Although significant, this regulatory framework was based on a minimum harmonisation model, leaving Member States a wide margin of discretion in its implementation.

---

[24] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 19; R. Mahari, T. Hardjono, A. Pentland, *AML by Design: Designing a Central Bank Digital Currency to Stifle Money Laundering*, MIT Science Policy Review, 3 (2023), at 58.; C. Westermeier, *The digital euro: a materialization of (in)security*, Review of International Political Economy 31 (V, 2024), p. 1575.

[25] C.-Y. Tsang *et al.*, *Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence*, cit., at 245.

[26] A. Adinolfi *et al.*, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, Quaderni AISDUE-Sezione Atti convegni AISDUE, 15 (2023), at 322-323; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Shaping Europe's Digital Future' COM(2020) 67 final.

[27] M. Niestadt, *The global reach of the EU's approach to digital transformation*, European Parliament - Briefing (2024).

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Subsequently, the Charter of Fundamental Rights of the European Union (CFREU)[29] expressly recognised, in Articles 7 and 8, the right to respect for private and family life and the right to the protection of personal data as autonomous fundamental rights, affirming principles that are binding both on European institutions and on Member States when implementing European law.

This normative evolution culminated in the adoption of Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR)[30], which marked a paradigm shift by introducing a uniform discipline directly applicable in all Member States. The GDPR strengthened the protection of personal data, placing emphasis on the principles of data minimisation, transparency, accountability, and privacy-by-design, imposing stringent obligations on both private entities and public authorities.

Although the European Union places strong emphasis on the protection of privacy, this right must, in any case, be balanced against the legitimate need to safeguard national security[31]. This delicate equilibrium between two potentially conflicting interests has been the subject of significant development in the case law of the Court of Justice of the European Union (CJEU). The Court has repeatedly affirmed that, while the rights enshrined in Articles 7 and 8 of the Charter are not absolute, any limitation must be provided for by law, respect the principle of proportionality, and pursue objectives of general interest or the protection of the rights and freedoms of others, in accordance with Article 52(1) CFREU[32].

In light of this regulatory and jurisprudential evolution, the protection of personal data now emerges not only as an individual right but also as a distinctive feature of the European model in the global context. These principles also underpin the approach adopted by the EU in the design of the digital euro[33], which is currently at the centre of a legislative process initiated with the proposal for a regulation presented by the European Commission on 28 June 2023[34] (hereinafter, the "Proposal").

---

[29] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[30] 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 [2016] OJ L119/1.

[31] L. Borlini, *Tutela della privacy e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del Sistema finanziario europeo*, Diritti Umani e Diritto Internazionale, 11 (I, 2017), at 24.

[32] See *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (Case C-623/17, CJEU, 6 October 2020); *Tele2 Sverige AB v Post-och telestyrelsen* (Joined Cases C-203/15 and C-698/15, CJEU, 21 December 2016) concerning the balancing of the right to data protection with national security interests; see also *Digital Rights Ireland and Others* (Joined Cases C-293/12 and C-594/12, CJEU, 8 April 2014) where the Court rendered Directive 2006/24/EC on data retention invalid.

[33] In line with the objective of creating a digital euro consistent with the democratic principles of the Union, the EDPB has highlighted the need to carry out a holistic assessment of the fundamental interests and rights involved – such as financial and digital inclusion, privacy protection, freedom of movement and security – to ensure that the design of the new digital currency is fully compliant with the founding values of the European legal system. See: EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro (2021).

[34] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final.

IV. The Proposed Regulation on the Digital Euro

The digital euro – still in the design phase – arises from the need to address the progressive digitalization of payment methods[35], strengthen the financial stability of the Eurozone, reduce dependence on private operators[36], and reaffirm the EU monetary sovereignty[37]. It will adopt a two-tier model, likely based on an intermediated architecture[38], whereby the European Central Bank (ECB) will directly issue the digital currency, while payment service providers (PSPs) will manage relationships with end users, providing wallets and payment services. The digital euro will not be programmable[39].

The digital euro aims to become an alternative (not substitutive) payment instrument to those already in existence, offering citizens a safe, accessible solution with a particular focus on the protection of privacy in digital payment transactions[40].

The importance given to this latter aspect is also reflected in the results of the public consultation conducted by the ECB[41], which revealed that 43% of participants – including citizens, businesses, and professionals – identified privacy as the main desired feature in the design of the digital euro. These concerns have been acknowledged by the ECB itself, which, from the beginning of the exploratory phase, emphasized that one of its core objectives is to identify design solutions capable of ensuring a high level of personal data protection and preventing potential risks for citizens, intermediaries, and the economy as a whole[42].

Consistently, the Proposal places data protection among the guiding principles of the initiative, explicitly referencing Article 8 CFREU of the European Union, the GDPR, and Regulation (EU) 2018/1725. In light of this, from the design phase onwards[43], the ECB and PSPs will be required to prioritize configurations that minimize the collection of personal data. These obligations have been formalized in Articles 34 and 35 of the Proposal.

In particular, the Proposal introduces specific obligations for PSPs to ensure that the processing of users' personal data fully complies with the principles of data minimization

---

35 F. Panetta, *Il costo di non emettere un euro digitale*, CEPR-BCE Conference (2023).

36 V. Lubello, *Central Bank Digital Currencies and the Digital euro: A Comparative Prism Between Sovereignty and Technology*. Itinerari della Comparazione, Scritti in onore di Giuseppe Franco Ferrari, 1 (2023), at 2.

37 P. Cipollone, Monetary sovereignty in the digital age: the case for a digital euro (2024), speech available at https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240927~11ed8493a4.en.html (last visited Jul 24, 2025).

38 In which the ECB will not have access to the register of all transactions. I. E. Linaritis, *Governance Issues Concerning the Issuer of CBDC, Who Supervises and Controls the CBDC Scheme?,* in Central Bank Digital Currency: The Birth of the Digital Euro (2025), at 196.

39 Programmability refers to the ability to embed conditions or restrictions directly into the digital currency itself, such as limiting its use to certain goods or services, defining a time period for its use, or specifying eligible recipients. This implies that the digital euro will not contain embedded features allowing public authorities to restrict its use for predefined purposes. There will be no technical mechanisms enabling the European Central Bank or governmental bodies to control how, when, where, or with whom digital euros can be spent. See FAQ on the digital euro, available at https://finance.ec.europa.eu/digital-finance/digital-euro/frequently-asked-questions-digital-euro-and-legal-tender-cash_en (last visited Jul 24, 2025).

40 F. Panetta, *Il costo di non emettere un euro digitale*, cit., at 9.

41 ECB, *Public consultation on a digital euro*, which was launched on 12 October 2020 and ran until 12 January 2021.

42 ECB, *Report on a Digital Euro* (2020).

43 In line with the principle of privacy-by-design codified at EU level by Art. 25 GDPR.

and purpose limitation[44], ensuring that the information processed is limited to the public interest purposes expressly set out in Article 34[45]. PSPs will need to adopt appropriate technical and organizational measures to ensure that the data processed are relevant and limited to what is necessary for the provision of payment services and for fulfilling regulatory obligations. PSPs are also responsible for adopting adequate technical and organizational measures to ensure that the data transmitted to the ECB and National Central Banks (NCBs) do not allow the direct identification of individual users[46].

Particularly stringent restrictions on access to personal data are imposed on the ECB and NCBs. Article 35 of the Proposal clarifies that the ECB and NCBs may only process data necessary to ensure the integrity, resilience, security, and operational continuity of the digital euro infrastructure, as well as to prevent fraud and cybersecurity incidents. In this context, processing must be carried out using pseudonymization techniques, encryption mechanisms, and separation of identifying information, in order to prevent the ECB and NCBs from being able to identify individual users[47].

Despite this regulatory framework, concerns have been raised in the literature about the risk that the proposed structure could still leave residual spaces for potential privacy violations, particularly by public authorities[48]. However, the CJUE, as mentioned, has already established the need to impose strict limits on government access to personal data, ruling that such access may occur exclusively for crime prevention purposes, subject to judicial authorization or independent review, and provided that the data are stored within the EU and permanently deleted at the end of the retention period[49]. It is reasonable to think that these limits may, in the future, also be applied to the digital euro.

Concerns similar to those raised in the literature have also been expressed by independent authorities, particularly the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), which, in their joint opinion of 2023, highlighted the risk that the creation of the single access point[50] provided for in Article 35(8) could lead to an excessive concentration of sensitive data, potentially enabling the identification of users by parties other than PSPs, in violation of the principles of data minimization and proportionality[51].

---

44 Recital 72.

45 Art. 34 (1) Proposal. On this point, the question arises as to whether the list is considered exhaustive or illustrative. See A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 13.

46 Art. 34(4) Proposal.

47 Art. 35(4) Proposal.

48 G. Soana, T. de Arruda, *Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture*, J. Bank Regul., 25 (2024), at 482-483; A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 16.

49 Joined Cases C-203/2015 and C-698/2015 (parr. 100 ff.; 120 ff.).

50 The single access point is a centralised technical infrastructure that allows PSPs to verify compliance with individual limits on the holding of digital euros by users. This system provides only aggregate responses (e.g. whether a given payment can be accepted without exceeding the limits) without allowing direct identification of users by parties other than the relevant payment service provider. The management of this infrastructure is entrusted to the ECB, possibly in conjunction with NCB, which are the controllers or joint controllers of the related personal data. See Recital 25 and Article 35(8) Proposal.

51 EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro (2023).

Consistently with the aim of maximizing privacy protection in the digital euro, the EDPB has also proposed[52] that the digital euro should replicate the features of cash, particularly in terms of privacy protection, adopting a threshold-based approach with proportional levels of anonymity depending on usage.

Coherently, the Proposal introduces the possibility of making offline payments in digital euros through hardware devices that do not require an internet connection: such transactions – largely assimilated to the use of cash or, more precisely, to ATM withdrawals[53] – are designed to offer a high level of privacy, ensured through data pseudonymization and the impossibility for the ECB, NCBs, and PSPs to access transaction details[54]. In this scenario, PSPs may only process data relating to the funding and defunding of accounts, but not data concerning peer-to-peer transfers[55].

For online payments, the Proposal provides for the application of the general principles on data protection and security, particularly the rules on anti-money laundering and counter-terrorist financing (AML/CFT). Online transactions will therefore be traceable in a manner similar to existing digital payment methods, and PSPs will remain subject to the reporting obligations under anti-money laundering regulations.

On this point, however, the joint opinion of the EDPB and EDPS expressed a significant reservation[56]. The two authorities regretted the European legislator's decision to exclude the adoption of a "selective privacy" regime even for low-value online payments. According to the supervisory bodies, the AML/CFT risk level for the online digital euro will largely depend on the technological and design choices made during the development phase. In this context, the introduction of risk mitigation measures could make it possible to extend the enhanced privacy regime provided for offline transactions also to low-value online payments. For this reason, the EDPB and EDPS strongly recommend that co-legislators consider introducing a threshold below which online transactions would not be subject to AML/CFT traceability, thereby ensuring a higher level of privacy aligned with user expectations.

The multi-layered architecture outlined by the Proposal thus appears to build an advanced balance between privacy protection and the security and transparency requirements of the payment system, even if some critical issues remain: beyond those already mentioned, the complexity of the proposed system – with the coexistence of different levels of data access and the need to ensure interoperability between public and private entities – could result in practical uncertainties and accountability risks[57].

In any case, the provisions appear consistent with the European approach to personal data protection and respond to the need to preserve user trust, which, as noted, is considered an essential condition for the widespread adoption of the digital euro.

---

52 EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro, cit..

53 Recital 71 Proposal.

54 Recital 71, Recital 82, articles 34 and 37.

55 Art. 37 Proposal

56 EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, cit..

57 A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 10.

Moreover, the extended timeline for the approval of the digital euro Regulation, combined with the careful analysis of privacy-related risks, is consistent with the prudential approach of the European legislator, traditionally committed to seeking regulatory solutions capable of effectively balancing personal data protection with the needs of financial system stability and security.

V. THE PEOPLE'S REPUBLIC OF CHINA APPROACH TO PRIVACY

The Chinese legal culture has always placed particular attention on notions such as public interest, national security, and social stability, values that are often considered to take precedence over individual rights[58]. This longstanding emphasis on these values has traditionally left limited room for the recognition of personal privacy as a legally protected right[59].

Starting from the 1980s, with the reforms promoted by Deng Xiaoping, the People's Republic of China (PRC) has witnessed a re-evaluation of the concept of privacy[60].

The evolution towards a market-oriented society and the growing legal transplantation of Western values[61] have indeed led to significant changes in the social perception of individual rights. The advent of new technologies has further encouraged the emergence of the individual as an autonomous subject with personal interests, while cultural opening has made discussions on issues such as personal freedom and individual rights, including the right to privacy, increasingly legitimate[62].

However, despite this evident cultural evolution and the enhancement of the legal protection of personal privacy compared to the past[63], scholars have highlighted that the Chinese approach to privacy continues to maintain a radical distinction from Western

---

[58] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 362; G. Ajani, A. Serafino, M. Timoteo, Diritto dell'Asia orientale (2007), at 53.

[59] See S. Peng, *Privacy and the Construction of Legal Meaning in Taiwan*, International Lawyer, 37 (IV, 2003), at 1039. H. Wang, *The conceptual basis of privacy standards in China and its implications for the China's privacy law*, Frontiers of law in China, 7 (2012), at. 137.

[60] H. Wang, *The conceptual basis of privacy standards in China and its implications for the China's privacy law*, cit., at 140-141; L. Yao-Huai, *Privacy and data privacy issues in contemporary China*, Ethics and Information Technology, 7 (2005), at 9. It should be noted that the traditional Chinese word for privacy, 阴私, historically carried a negative connotation, often referring to shameful or immoral secrets, and therefore was not adopted into legal discourse (see M. Xu [徐明], *Privacy Crises in the Big Data Era and Responses under Tort Law*, [大数据时代的隐私危机及其侵权法应对], China Law [中国法学] 1 (2017)). The word that translates the western concept of privacy is 隐私 (see G. Zhu, *The Right to Privacy: An Emerging Right in Chinese Law*, Statute Law Review, 18 (III, 1997), at. 208).

[61] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 373-374; G. Ajani, A. Serafino, M. Timoteo, Diritto dell'Asia orientale, cit., at 306 ff.

[62] Lu Yao-Huai, *Privacy and data privacy issues in contemporary China*, cit., at 11.

[63] Already in 1982, the Chinese Constitution recognized certain privacy-related rights, such as personal dignity (art. 38), personal freedom and residence (arts. 37 and 39), and the confidentiality of correspondence (art. 40). Article 101 of the 1986 General Principles of Civil Law established the right to reputation for individuals and legal entities, prohibiting insults, defamation, and other acts that harm personal dignity. In 1988 the Supreme People's Court issued a legal interpretation clarifying that publicly disclosing someone's private information constitutes a violation of their right to reputation and may give rise to civil liability (法 [办] 发 [1988]6 号《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见（试行）》).

models: in the Chinese perspective, the protection of privacy remains strongly anchored to the centrality of collective interests and public order[64].

Not even the adoption of dedicated legislation on personal data protection, namely the *Personal Information Protection Law* (PIPL)[65], nor the inclusion of privacy within the personality rights of the Chinese Civil Code[66], seem to have altered this trend. On the contrary, it has been observed that the introduction of privacy regulations in the PRC takes on a strongly public dimension[67]. In fact, the widespread public discontent arising from personal data breaches has pushed the regulator to officially recognize privacy invasions as potential sources of social instability[68].

Additionally, the strategy adopted by the regulator has not resulted in a limitation of public surveillance but rather in a reinforcement of its role as the citizens' protector against abuses perpetrated by third parties. The legislative action has allowed the leadership to present itself as the primary defender of privacy, without however questioning the prerogatives of state control[69]. In this narrative, privacy violators are never identified as the authorities themselves but rather as external actors such as greedy companies or fraudsters[70]. This framework seems to reflect a recurring pattern in Chinese governance, characterized by a notable asymmetry between the stringent restrictions placed on private actors and the wide discretionary powers afforded to public authorities[71].

In this context the development of the e-CNY takes place. The digital yuan not only represents a technological advancement in the payment system but also constitutes an instrument through which multiple objectives are pursued: from promoting innovation and economic efficiency to ensuring more effective supervision of financial transactions, as well as advancing the internationalization of the RMB. The e-CNY thus stands at the crossroads of digitalization, security needs, and privacy protection objectives, according to an approach that reflects the distinctive features of the Chinese system.

---

64 Lu Yao-Huai, *Privacy and data privacy issues in contemporary China*, cit., at 11.

65 Personal Information Protection Law [中华人民共和国个人信息保护法], promulgated by the Standing Committee of the 13th National People's Congress on August 20, 2021, effective November 1, 2021.

66 Book 4, Personality Rights, Chinese Civil Code [中华人民共和国民法典], promulgated by the 13th National People's Congress on May 28, 2020, effective January 1, 2021.

67 M. Jia, *Authoritarian Privacy*, University of Chicago Law Review, 91 (2024).

68 This is mentioned, for example, in the "*Notice Relating to Performing Good Work During New Year's Day and the 2021 Spring Festival*" issued by the General Office of the Chinese Communist Party Central Committee and the State Council General Office (中共中央办公 厅 国务院办公厅印发《关于做好 2021 年元旦春节期间有关工作的通知》).

69 E. Toti, *Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC "con caratteristiche cinesi"*, Rivista di Diritto dei Media (I, 2023), at 212.

70 Mark Jia, *Authoritarian Privacy*, cit., at 737; this perspective appears to align with the Chinese approach to the rule of law "with Chinese characteristics", a model in which law is subordinated to the leadership of the Communist Party and serves primarily as an instrument for achieving policy goals. For a more in-depth discussion on this topic, see: G. Ajani, *La Rule of Law in Cina*, Mondo Cinese, 126 (2006); I. Castellucci, Rule of Law and Legal Complexity in the People's Republic of China (2012).

71 R. Cavalieri, *La legalità socialista di Xi Jinping*, Tra storia e politica. L'Asia orientale contemporanea e il contributo di Enrica Collotti Pischel (2024), at 107.

VI. THE DIGITAL YUAN

Although Chinese authorities have been focusing on the topic of CBDCs for over a decade[72], there is currently no specific regulation concerning the digital yuan in the PRC, nor concerning privacy protection in this field[73]. Furthermore, no case law on the matter has been recorded. Therefore, the legal analysis must rely on non-binding rules and on the existing legal framework for personal data protection as provided in the Civil Code and the PIPL.

From an operational standpoint, as outlined in the White Paper issued by the People's Bank of China (PBOC) in 2021[74], the e-CNY is based on a two-tier system in which the PBOC retains control over the issuance and central management of the currency, while distribution and interaction with end users are entrusted to private entities, such as commercial banks and authorized payment platforms. Unlike the digital euro, the PBOC also maintains the ledger of all transactions carried out in e-CNY, making it a hybrid model where the operational management is delegated to intermediaries, but the control over the transaction flows remains centralized with the monetary authority[75].

The digital yuan is programmable, and the system's architecture is inspired by the principle of "managed anonymity", according to which low-value transactions have a higher degree of anonymity, while high-value transactions are fully traceable[76]. The e-CNY is stored in different types of wallets, each offering varying levels of anonymity and spending limits. Wallets are classified based on the degree of identification required: those with less stringent requirements allow low-value payments (up to a maximum of 2,000 CNY per transaction) and can be accessed with just a phone number registration[77].

At first glance, this structure – similar to that of the EU, as it consists of a hybrid model between account-based and quasi-account-based systems [78] – presents, however, significant differences in terms of privacy: low-value transactions, which are comparable to offline payments in the digital euro project, do not offer the same levels of anonymity, since the Chinese wallet is always mandatorily linked, as mentioned, to a phone number

---

[72] The first studies on the creation of a national CBDC date back to 2014. Attention turned more to the issue in 2019, as a way of countering crypto-assets and stablecoins, which had already been banned since 2017 and then expanded. See PBOC, *Progress of Research & Development of E-CNY in China*, Working Group on E-CNY Research and Development of the People's Bank of China (2021), at 1.

[73] Despite this, scholars have repeatedly highlighted the need for clear and comprehensive regulations in this area, and the same point was made by the authorities in the white paper. See: Y. Chen, M. Adams, *The Regulation of Digital Currency in China: Past, Present, and Future*, European Journal of Law Reform, 25 (I-II, 2023), at 159; PBOC, *Progress of Research & Development of E-CNY in China*, cit., at 11.

[74] PBOC, *Progress of Research & Development of E-CNY in China*, cit..

[75] This means that the central bank can keep a copy of retail balances and transactions, giving the PBOC full, centralised access to detailed data on each user's accounts and transactions, regardless of the intermediary used. See: J. Jiang, *supra*, at 117.

[76] PBOC, *Progress of Research & Development of E-CNY in China*, cit., at 7.

[77] See Guangzhou Huadu District Financial Work Bureau [广州市花都区金融工作局], Mu Changchun of the Central Bank explains the four types of digital RMB wallets in detail, [央行穆长春详解四类数字人民币钱包] (2021).

[78] Z. Li, J. Li, 2025. *Evaluating the Wallet-Based DCEP: Regulatory Innovations and Implementation Strategies in China's Retail CBDC*, Laws 14 (III, 2025), at 4. It should be noted that high levels of anonymity are provided by the so-called value-based category, which are hardware devices that contain digital yuan without being linked to a bank account (examples include prepaid cards or transport cards).

which, in turn, is tied to an identity card[79]. Even though the European model also requires some form of identification, strict limits are imposed on the use of data related to these transactions[80]. The absence of similar provisions in the Chinese context increases the risk that even low-value operations may be subject to systematic tracking and profiling.

Reflections on this CBDC model, when read in light of the privacy-by-design principle, make the e-CNY a paradigmatic example of how the technical infrastructure of a digital currency can itself serve as a policy tool, translating political goals into operational solutions through the CBDC's design[81]. Unlike the European project, where the Proposal explicitly imposes limitations on data access by the ECB, NCBs, and PSPs – constraints that must necessarily be embedded in the technical infrastructure through specific engineering solutions – the absence of equivalent legal safeguards in the PRC[82] raises the risk that the e-CNY infrastructure may allow for unlimited processing of users' financial information, with clear concerns in terms of privacy protection and transparency[83].

Even the existing personal data protection framework does not seem adequate to protect users from potential abuses for two main reasons: *(i)* firstly, because *ex post* regulation does not provide the same level of protection as that which is embedded directly within the technical infrastructure; *(ii)* secondly, because the Chinese privacy framework contains room for interpretation that could, in practice, significantly broaden the authorities' powers to access personal data.

Regarding the first point, it has been observed that existing privacy laws offer protective measures that operate downstream and are thus secondary, whereas embedding personal data protection directly into the infrastructure is more effective than sanction-based, *ex post* interventions[84].

---

[79] Y. Chen, M. Adams, *The Regulation of Digital Currency in China: Past, Present, and Future*, cit., at 156; article 24 Cybersecurity Law (中华人民共和国网络安全法).

[80] As discussed in section IV, PSPs will only be able to process essential information related to the funding and defunding of funds, without being able to access data relating to transactions between users. Furthermore, pursuant to recital 71 and Article 37(2), neither the ECB nor the national central banks may attribute the data to an identified or identifiable user of the digital euro. A partial exception in this regard is provided for in Article 37(3), which requires PSPs to make user data available in cases of suspected money laundering or terrorist financing.

[81] C. Xu, B. Jin, *Digital currency in China: pilot implementations, legal challenges and prospects*, Juridical Tribune 12, (II, 2022), p. 185.

[82] Article 51 PIPL, which can be regarded as the provision closest to a codification of the privacy-by-design principle within the Chinese legal framework, nonetheless differs from Article 25 GDPR insofar as it does not establish such an approach as a general design principle, but rather as a set of operational obligations aimed at ensuring the security of processing. Partially complementing Article 51 is the Information Security Technology – Personal Information Security Specification (信息安全技术个人信息安全规范), which appear, in Article 11.2, to set out an *ex ante* requirement for the development of systems that ensure privacy protection. However, this document is non-binding in nature.

[83] C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, cit., at 185-186.

[84] J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 130.

As for the second point, it seems that the general personal data protection framework formally applies to the e-CNY as well[85]. This framework is characterized by a "dual" structure, as it is divided between the Civil Code and the PIPL[86].

Both sources seem to recognize that financial information falls within the category of protected personal data[87]: therefore, transactions conducted through e-CNY would also appear to fall within this category. Since this information qualifies as personal data, it should, at least in principle, be protected against potential misuse, both by private entities and by public authorities. The Chinese legal framework, indeed, seems to place public and private actors on the same level, following what has been defined as a unitary legislative model[88]; however, the legislation includes broad exceptions aimed at safeguarding public interests.

In this context, all data controllers – whether authorities[89] or commercial banks – are, at least in theory, required to comply with the provisions of the PIPL, which imposes strict limits on the collection, use, and storage of users' data, and requires the implementation of appropriate technical and organizational measures to ensure the security and confidentiality of the processed information[90]. In particular, the law requires that personal data be processed lawfully, fairly[91], and when necessary, following the principles of minimization and specific purpose limitation[92].

However, as mentioned, Chinese regulation – consistently with the traditional approach to privacy outlined above – recognizes significant exceptions to these general principles

---

85 X. Chen, *Privacy Protection in the Context of CBDC: Development Trends and China's Practice*, J. East Asia & int'l l., 16 (II, 2023); J. Jiang, L. Lucero, *Background and implications of China's e-CNY*. University of Florida Journal of Law and Public Policy, 33 (II, 2023), at 265.; C. Mu, *Theories and practice of exploring China's e-CNY, Data, Digitalization, Decentralized Finance and Central Bank Digital Currencies: The Future of Banking and Money*, cit., at 185.

86 D. Clementi, *La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?*, Rivista di Diritti Comparati (2022). As highlighted by the author, the Civil Code and the PIPL protect, respectively, the autonomous rights to privacy and personal information: the former is seen as a "negative" right to prohibit intrusion into private life; the latter is seen as a positive right, which values the right to control who uses one's personal information. For a general overview of the PIPL, see B. Verri, *The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL)*, in M. Timoteo, B. Verri, R. Nanni (eds.), Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China (2023).

87 The financial data would in fact fall within the scope of Article 1034 of the Civil Code and the combined provisions of Articles 4 and 28 PIPL.

88 Y. Wang [王怡坤], *A Research on the Legitimacy Standard of Personal Information Processing Behaviors by State Organs* [国家机关个人信息处理行为正当性标准研究], China L. Rev. [中国法律评论] 42 (VI, 2021).

89 Art. 33 PIPL.

90 However, Chinese scholars have raised some concerns about the effective protection of personal data by the banking institutions involved in managing e-CNY wallets. In particular, it has been noted that when downloading the digital yuan app, users are required to accept the specific privacy policies set by individual commercial banks, without which the wallet cannot be opened. However, these policies vary significantly between different banks and, in some cases, require users to provide personal data that appears to exceed the minimum requirements of current legislation. See: W. Wang [王炜炫], *Personal Information Protection in the Issuance and Circulation of Digital RMB* [数字人民币发行和流通中的个人信息保护], Southern Finance [南方金融], 562 (2023). This critical issue does not contradict the fact that banks are subject to stringent obligations regarding the protection of personal data. On the contrary, it highlights a possible disconnect between the formal regulatory framework and its application in practice, which requires legislative intervention to standardise the conditions for opening wallets.

91 Art. 5 PIPL.

92 Art. 6 PIPL.

when necessary to protect public interests. Article 1036 of the Chinese Civil Code provides for an exemption from civil liability when personal data is processed for the protection of the public interest.

Consistently, Article 13 of the PIPL allows the processing of personal data without the data subject's consent when such processing is necessary for the exercise of public functions, for purposes of public interest, for the protection of health, for journalistic activities, or for public opinion supervision.

Although such exceptions seem to be justified, particularly from the perspective of Chinese scholars[93], by the need to combat crimes that may jeopardize social stability, the vagueness and ambiguity of the terminology used in the legislation – especially references to generic concepts such as the public interest or public opinion supervision – risk creating significant areas of legal uncertainty, resulting in a substantial erosion of privacy guarantees[94].

This legal uncertainty appears, in fact, to be a recurring feature of the Chinese legal system[95], which inevitably leads to a certain degree of flexibility in interpretation and application of law on a case-by-case basis. Such vagueness becomes particularly problematic in the context of the digital yuan, where financial data can notoriously reveal with great accuracy spending habits, individual preferences, and deeply personal aspects of a person's identity.

In light of these considerations, the legal and technical architecture of the e-CNY seems to confirm the existence of a governance model that is strongly focused on the protection of public interest and the safeguarding of social stability, where privacy protection, although formally acknowledged, appears structurally subordinated to widespread control needs. The absence of specific regulation for the digital yuan and of strict legal safeguards limiting public authorities' access to data, combined with the broad exceptions provided in the general data protection framework, ultimately may contribute to an imbalanced system in which end users have limited avenues to challenge potential misuse of their data.

In this sense, the digital yuan seems to be a clear example of a governance model of CBDC "with Chinese characteristics" (中国特色), reflecting a balance between privacy and public interest that is profoundly different from the one emerging in the European context.

Against this backdrop, future research should closely monitor how the Chinese legal system will concretely operationalize its data protection principles in the context of the digital yuan, particularly in relation to the role of courts in addressing potential rights violations.

VII. The Brussels Effect and the Beijing Effect in the field of CBDCs

This paper has examined the divergent governance and design models of CBDCs through a comparative lens, highlighting the emergence of distinct regulatory paradigms: these

93 X Chen, *Privacy Protection in the Context of CBDC: Development Trends and China's Practice*, cit., at 229.
94 J. Jiang, L. Lucero, *Background and implications of China's e-CNY*, cit., at 267.
95 D. Cao, Chinese Law: A Language Perspective (2004), at 94 ff.; P. B. Potter, The Chinese Legal System: Globalization and Local Legal Culture (2001), at 11; E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, Penn. St. J.L. & Int'l Aff., 8 (2020), at 74; B. Verri, *The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL)*, cit., at 195.

models could also be replicated in other jurisdictions, given the need, as mentioned, to create common standards for cross-border payments.

The absence of a consolidated global regulatory model for CBDCs offers the European Union a valuable opportunity to establish itself as a leader in the definition of such standards[96], potentially influencing the regulatory choices of other jurisdictions. The European Union, already a key player in the global standard-setting process through the phenomenon known as the Brussels Effect[97], is well positioned to extend its influence on the field of CBDCs as well[98]. In this sense, the adherence of third countries to European standards may become a necessary condition for achieving the interoperability objectives mentioned above, especially where these countries wish to ensure compatibility between their CBDC systems and the European one.

The EU regulatory influence in this context could be exercised for two principal reasons: *(i)* firstly, because it satisfies the conditions identified by Anu Bradford for the emergence of the Brussels Effect, combining a large consumer market with a high regulatory capacity and a strong political will to impose stringent rules. Moreover, the CBDC domain targets relatively inelastic users (such as citizens and businesses) and relies on technological infrastructures that cannot be easily segmented across jurisdictions, given the need for a common framework to ensure interoperability between different CBDCs; *(ii)* secondly, due to the central role that privacy protection plays in the perception and acceptance of CBDCs by both citizens and businesses. Indeed, the demand for digital payment instruments is increasingly shaped by users' sensitivity to the processing of personal data, and it is reasonable to expect that citizens and businesses will prefer to use CBDCs – rather than alternative digital payments – only where such instruments effectively safeguard their privacy[99].

Finally, it should be noted that, in the context of CBDCs, the need to apply uniform standards does not concern PSPs alone but also central banks and public authorities more broadly. In this regard, a mere *de facto* adaptation by PSPs located outside the EU to European standards would not be sufficient to ensure genuine regulatory convergence. Only through a formal harmonization of domestic legal frameworks in line with European principles (*de jure* alignment) can full legal interoperability between CBDC systems be guaranteed.

Unlike the European Union, whose potential influence in the CBDC domain could materialize through regulatory projection based on the Brussels Effect, the international influence of the PRC may develop according to profoundly different logics.

---

[96] C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, cit., at 187 emphasises the importance of creating a global regulatory framework.

[97] A. Bradford, The Brussels Effect: How the European Union Rules the World, cit..

[98] F. Panetta, *The present and future of money in the digital age*, ECB (2021), available at: https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211210~09b6887f8b.en.html (last visited Jul 24, 2025).

[99] F. Tronnier, W. Qiu, *How do privacy concerns impact actual adoption of central bank digital currency? An investigation using the e-CNY in China*, Quantitative Finance and Economics, 8 (I, 2024); S. Choi *et al.*, *Central Bank Digital Currency and Privacy: A Randomized Survey Experiment*, BIS Working Papers (2023); F. Tronnier *et al.*, *Investigating privacy concerns and trust in the digital Euro in Germany*, Electronic Commerce Research and Applications, 53 (2022).

It is worth noting that although China was long considered a rule-taker, generally inclined to adopt external norms[100], this approach has shifted in recent decades. China has gradually moved away from the role of mere recipient of standards developed by other jurisdictions to become an active rule-maker, particularly in emerging technological sectors[101].

This shift has been particularly evident since 2013, with the launch of the Belt and Road Initiative (BRI)[102], which therefore constitutes a unique standpoint for analysing China's international projection strategies. The BRI, introduced under Xi Jinping's presidency, is a global strategy aimed at building infrastructure and promoting a new China-centered model of globalization. Through massive investments in Eurasia and other strategic regions, China seeks to consolidate its sphere of influence, not only through economic and industrial advantages but also by exporting its own standards, norms, and values[103].

A particularly significant component of this strategy is the Digital Silk Road, the BRI's branch dedicated to investments in information and communication technologies[104]. Through these projects, China is not merely expanding its economic and political presence but is actively promoting the adoption of its technological architectures and imposing the use of Chinese technical standards. This dynamic has produced considerable effects: the diffusion of Chinese technological infrastructures prompts private operators and third countries to adopt compatible standards to ensure system interoperability[105], thereby consolidating PRC influence in the digital sphere and reinforcing the global penetration of Chinese standards.

In addition to this mechanism of exporting technological standards, PRC also exerts an attractive influence through its model of data sovereignty, which is characterized by strong centralization and the clear subordination of private operators to public objectives[106].

This model of influence has been described in scholarly literature as the Beijing Effect, in contrast to the aforementioned Brussels Effect[107]. Unlike the latter, which is based on the normative influence of European rules, PRC influence is not expressed through the direct projection of legal norms[108] but rather – as noted – through the export of a data

[100] China's transplantation of legal models has not occurred through a mere transposition of foreign legal frameworks in its legal system, but rather through a selective adaptation of external legal standards to its own socio-cultural and political context. See P. B. Potter, The Chinese Legal System: Globalization and Local Legal Culture, cit., at 4; D. Zoppolato, P. D. Farah, *China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative*, Asian Journal of Law and Society (2025), at 3 ff.

[101] R. Cavalieri, *La legalità socialista di Xi Jinping*, cit., at 107; H. Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, Journal of International Economic Law, 23 (2020), at 584.

[102] *Id*., at 584; D. Zoppolato, P. D. Farah, *China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative*, cit., at 2.

[103] M. Simonov, *The belt and road initiative and partnership for global infrastructures and investment: comparison and current status*, Asia and the Global Economy (2025), at 2

[104] F. Klein, N. Baker, *China and its Central Bank Digital Currency – Is the E-Yuan a Role Model for Europe and the Euro System?*, Friedrich Erbert Stifung (2023), at 6

[105] M. S. Erie, T. Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance,* N.Y.U. J. Int'l L. & Pol., 54 (I, 2021), at 23.

[106] *Id*, at 21.

[107] *Id*, at 17-20.

[108] Indeed, this could hardly be the case: China's regulatory capacity and expertise still face certain limitations, particularly with regard to the extraterritorial application of its laws. See A. Bradford, Digital empires: the global battle to regulate technology (2023), at 328-329. Unlike the European Union, China has never sought to adopt extraterritorial regulations as a means of projecting its influence abroad, in line with its traditional anti-hegemonic stance. Only in recent years has China shown a tendency towards extraterritoriality, with the

governance model and the dissemination of technological standards that gradually become established in international markets[109].

In light of this reconstruction, it cannot be excluded that this model could also extend to the realm of CBDCs. In fact, the inherently technological nature of CBDCs and the need to ensure interoperability between different digital payment systems may represent a particularly favourable channel through which the Beijing Effect could operate.

Given that many BRI countries often lack adequate financial infrastructures, it is likely that they will collaborate with Chinese financial institutions to develop their own CBDCs. In this context, it is plausible that the governments of these countries will rely not only on Chinese technologies but also on Chinese policies concerning CBDCs[110]. Furthermore, it seems reasonable to expect that these countries may gradually emulate the Chinese model of financial data governance, converging towards practices of managed anonymity and traceability of financial flows. In these terms, the Beijing Effect could materialize.

In addition to this perspective, an emerging strand of scholarship has emphasized PRC influence over other jurisdictions by framing it within a broader paradigm of digital authoritarianism, characterized by pervasive surveillance practices, infrastructural control, and restrictions on the autonomy of private actors[111]. According to some authors, the design and governance of CBDCs could serve as a vehicle for the extension of this model to other jurisdictions. Specifically, this doctrine highlights that the regime of managed anonymity reflects an authoritarian conception of privacy, which may have the potential to influence other authoritarian regimes transnationally[112].

The analyses presented here ultimately suggest that, despite the absence of a comprehensive and systematic regulatory framework for the digital yuan that could be replicated as a normative model by other jurisdictions, PRC has nonetheless succeeded in positioning itself as a central actor in the international CBDC discourse. This outcome has been facilitated both by PRC first-mover advantage, gained through the early introduction and advanced experimentation of the e-CNY, and by its active participation in key standard-setting bodies, where it contributes to the development of guiding principles for CBDCs[113].

PIPL representing a significant step in this direction. See W. Cong., *The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics*, in M. Jiang, L. Belli (eds.), Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance (2025), at 79.

[109] *Id*, at 23.

[110] C.-Y. Tsang, P.-K. Chen, *Policy Responses to Cross-Border Central Bank Digital Currencies – Assessing the Transborder Effects of Digital Yuan*, Capital Markets Law Journal, 17 (2022), at 250.

[111] A. Polyakova, C. Meserole, *Exporting digital authoritarianism*, Brookings Institute Foreing Policy Reports (2019). On the topic see also: X. Qiang, *Chinese Digital Authoritarianism and Its Global Impact*, in Digital Activism and Authoritarian Adaptation in the Middle East (2021), available at https://pomeps.org/chinese-digital-authoritarianism-and-its-global-impact (last visited Jul 25, 2025); A. Liaropoulos, *Digital Authoritarianism "Made in China": Installing a Digital Dystopia*, National security and the future, 23 (I, 2022); D. Lilkov, *Made in China: Tackling digital authoritarianism*, European View, 19 (I, 2020).

[112] N. Kshetri, *China's Digital Yuan: Motivations of the Chinese Government and Potential Global Effects*, Journal of contemporary China, 32 (2023), at 103.

[113] H. Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, cit., at 593.

In conclusion, the PRC may exert significant influence in the future, predominantly of a technical and infrastructural nature, in shaping the global CBDC ecosystem, promoting a model that is no longer primarily regulatory, but rather technical and governance-oriented.

VIII. CONCLUSIONS

The comparative analysis conducted in this work developed from the identification of a problem shared by multiple legal systems: the need to design CBDCs that combine the efficiency and security of payments with an adequate level of privacy protection for citizens. This common issue has constituted the starting point for an investigation aimed at examining the concrete solutions adopted (albeit in an evolving context) by two of the main economic actors on the global stage.

This balancing exercise is inevitably situated within the social, cultural, and political framework of each legal system. The analysis of the EU and the PRC models have shown that the design of CBDCs reflects implicit cultural structures – the so-called cryptotypes[114] – that profoundly influence regulatory choices. The differing conceptions of the relationship between public authority and the individual, and of the function of personal data protection, are manifested in the distinct technical and legal architectures of the respective CBDCs.

What emerges is that the European model is characterized by a strong *ex ante* and *ad hoc* regulatory framework, which seeks to embed the fundamental principles of the European legal order within the technical and design choices of the CBDC. By contrast, the Chinese model appears to allow a relatively broad degree of discretion in shaping the technical infrastructure and, as a result, in managing data, in the absence of a detailed and binding regulatory framework.

The analysis of the divergences and convergences between these models made it possible not only to highlight their underlying rationales, but also to suggest potential future trends in the global regulation of CBDCs. Indeed, a jurisdiction's approach to privacy in the context of CBDCs can influence other States[115], potentially guiding the emergence of shared practices and new international standards in their design and regulation.

As noted at the outset of this contribution, the efficiency of CBDCs will largely depend on their ability to be employed in cross-border transactions, which presuppose not only technical but also legal interoperability. From this perspective, it is evident that regulatory harmonization – particularly in the field of personal data protection, but not exclusively – is not only desirable but in fact essential[116].

The European Union, which already plays a central role in shaping global regulatory standards through the Brussels Effect, appears well placed to extend this influence on the emerging field of CBDCs. At the same time, the PRC, as noted, can positions it as a potential influencer of other legal systems, leveraging its geopolitical network through the BRI, and on its first-mover advantage in a field devoid of common standards.

---

114 A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 6.

115 H. Wang, *Understanding Disputes Over Digitalization: A Perspective of Cross-Border Central Bank Digital Currencies* (2025), at 16.

116 BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 25.

How these models will interact, compete, or converge on the international stage remains to be seen. What is certain, however, is that the choices made today by key global actors will have long-lasting implications for the governance of digital money and the protection of individual rights in the digital age.