Understanding Transaction Data Privacy in CBDCs: A Rights-Based Framework

Abstract

In the digital age, Central Bank Digital Currencies (CBDCs) have been introduced as a response to the growing use of private money and crypto-assets while preserving the anchoring role of central bank money. Realising these benefits, however, requires a degree of visibility over transaction data that privacy laws and constitutional principles do not always permit, creating tension between financial integrity and the protection of individual privacy. Against this background, this paper examines how the law should respond to privacy concerns surrounding CBDCs by analysing the rights engaged by transaction data. Focusing on China's e-CNY and the EU's digital euro, it argues that the protection of CBDC transaction data encompasses both the right to privacy and the right to personal information. Building on this analysis, the paper draws on Daniel J. Solove's taxonomy of privacy to argue that, from the perspective of the right to privacy, both China and the EU should place greater emphasis on regulating the use of transaction data after collection. Central banks should be granted authorisation for specific purposes to process transaction data, rather than broad authorisation covering all circumstances except those expressly prohibited. Furthermore, during the dissemination of data, recipients should be subject to strict regulation to prevent the unauthorised dissemination. From the perspective of the right to personal information, the paper further draws on Helen Nissenbaum's theory of contextual integrity to argue that transaction-amount-based visibility mechanisms should also take account of the sensitivity of transaction data. It further proposes organisational separation and data isolation between institutions to prevent excessive dissemination and use of transaction data, thereby strengthening individuals' control over their personal information.

Keywords: central bank digital currencies (CBDCs), privacy rights, personal information rights

Introduction

Cash is rapidly disappearing from everyday life, with credit cards and mobile payment platforms increasingly dominating retail transactions. According to the European Central Bank's (ECB) statistics, contactless payments now account for 79% of everyday payments.[1] Coupled with the rapid development of crypto-assets, these developments have intensified concerns that physical central bank money may gradually be squeezed out. In response, many jurisdictions have accelerated the development of Central Bank Digital Currencies (CBDCs) to preserve the uniformity and effective use of central bank money in the digital economy.[2] According to a survey conducted by the Bank for International Settlements (BIS) covering 93 central banks, 91% of respondents are currently exploring CBDCs, including both retail and wholesale models.[3] Whilst retail CBDCs are intended primarily for everyday transactions between individuals, wholesale CBDCs are designed mainly for large-value transfers between financial institutions. As this paper focuses on data protection issues arising from the use of CBDCs by individuals, it focuses exclusively on retail CBDCs.[4]

As a digital form of central bank money, CBDCs provide a digital equivalent of legal tender, thereby preserving the anchoring role of central bank money within the monetary system and mitigating potential risks to financial stability. Achieving these objectives, however, requires a certain degree of visibility over transaction data, which privacy laws and constitutional principles do not always permit.[5] As revealed by the European Central Bank (ECB) survey, privacy is regarded by 41% of respondents as the most important feature of a digital euro.[6] This creates a potential tension between the use of CBDCs to strengthen financial integrity and the protection of individual privacy.

The issue has attracted increasing attention from both policymakers and academic researchers. Currently, most research on privacy protection in CBDCs discusses

---

[1] European Central Bank, 'Payments Statistics: First Half of 2024', European Central Bank, 2024, https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h1~5263055ced.en.html, accessed 12 December 2025.

[2] 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 (28 June 2023).

[3] Bank for International Settlements, 'Results of the 2024 BIS Survey on Central Bank Digital Currencies' (2025) https://www.bis.org/publ/bppdf/bispap159.pdf accessed 12 December 2025.

[4] Alexandros Roussou and others, 'Central Bank Digital Currencies: A Critical Review' (2024) International Review of Financial Analysis 103705.

[5] Lianchao Chen, 'Central Bank Digital Currencies and State Capitalism in China: The Institutional Hybridity of the E-CNY' (2026) 171 Geoforum 104601.

[6] Syngjoo Choi and others, 'Central Bank Digital Currency and Privacy: A Randomized Survey Experiment' [2022] SSRN Electronic Journal.

'privacy' or 'data protection' as broad concepts, without specifically analysing which rights are actually involved in CBDCs privacy protection: the right to privacy, the right to personal data, or both. This analysis is important because these rights, although overlapping in practice, rest on different normative foundations and are governed by different legal rationales. Before considering how privacy should be protected in the context of CBDCs, it is therefore necessary to clarify which rights are involved and how privacy should be understood in relation to CBDC transaction data.

Accordingly, this article examines how the legal framework should protect CBDC transaction data from the perspective of the rights involved. It takes China's e-CNY and the EU's digital euro as case studies, as they represent the two most advanced large-scale CBDC projects and provide valuable guidance for jurisdictions developing their CBDCs. Following this introduction, Section I introduces the e-CNY and the digital euro and analyses their principal privacy concerns, including potential state surveillance arising from central bank access to transaction data and the excessive collection of personal information by commercial banks and other authorised institutions. Section II examines the rights engaged by CBDCs transaction data from the perspective of the philosophical foundations of the right to privacy and the right to personal information. It argues that the protection of CBDC transaction data encompasses both rights, with the former centred on protecting individuals' transactional autonomy and the latter on preserving individuals' control over their personal information.[7] Building on this analysis, Section III develops separate legal recommendations for the protection of each right. With respect to the right to privacy, drawing on Daniel J. Solove's taxonomy of privacy, the paper argues that both China and the EU should place greater emphasis on regulating the processing, dissemination and other post-collection uses of transaction data.[8] In particular, the purposes for which central banks may process transaction data should be interpreted narrowly, and the disclosure of transaction data should be subject to strict restrictions on authorised recipients. With respect to the right to personal information, the paper argues that the current transaction-amount-based data visibility framework adopted by both jurisdictions should be refined by also taking account of the sensitivity of transaction data.[9] It further proposes the establishment of a strict system of organisational separation and data isolation to prevent unnecessary dissemination of transaction data to unrelated parties without users' effective control.

---

[7] Julie E Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (Yale University Press 2012). Alan F Westin, Privacy and Freedom (Atheneum 1967).
[8] Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154(3) University of Pennsylvania Law Review 477.
[9] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) Washington Law Review 119.

I. The e-CNY and the Digital Euro: Privacy Concerns

1.1 Introduction to the e-CNY and the digital euro

Firstly, China's CBDC is known as the e-CNY.[10] As defined by the People's Bank of China (PBOC), the e-CNY is 'the fiat currency issued by the central bank.'[11] The e-CNY's status as fiat currency means that it is legal tender and constitutes a claim on the PBOC. Concerning privacy protection for the e-CNY, China has primarily adopted a two-tier structure and controlled anonymity. Under the two-tier structure adopted by the e-CNY, different data management responsibilities are allocated amongst the PBOC and other designated operating institutions, including commercial banks, and they have varying levels of data visibility, thereby reducing the central bank's direct control over user data. The controlled anonymity design relies primarily on a mechanism of anonymity for small transactions and traceability for large transactions. Currently, the e-CNY comprises four wallets, each with different transaction amount limits and levels of data visibility. The Tier 4 wallet can be opened with just a mobile phone number and is claimed to offer the strongest privacy protection. Commercial banks can only see users topping up and withdrawing e-CNY, and cannot track subsequent spending patterns. Correspondingly, it has the lowest payment limit, with a current balance cap of 10,000 yuan (approximately 1,200 euros).[12] Tier 4 wallets have the highest transaction limits, with no explicit regulations currently in place regarding daily or per-transaction limits. Users are subject to the strictest data disclosure requirements; to use a Tier 4 wallet, they need to provide personal information in a manner approaching full real-name verification.[13]

Secondly, the digital euro is a digital form of the euro issued by the European Central Bank (ECB).[14] It is necessary in a context where European payment systems are becoming increasingly digitalised, the use of cash is declining significantly, and foreign CBDCs or private digital payment instruments, including stablecoins, may be

---

[10] Heng Wang, 'How to Understand China's Approach to Central Bank Digital Currency?' (2023) 50 Computer Law & Security Review 105788 https://doi.org/10.1016/j.clsr.2022.105788.

[11] People's Bank of China, 'Progress of Research and Development of E-CNY in China' (White Paper, July 2021) 3 <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf> accessed 20 April 2025.

[12] Securities Times, 'Strongly Identified Wallets Have No Limits: A Detailed Examination of the E-CNY Wallets Offered by Seven Operating Institutions' [《强实名类钱包不限额，详解 7 家运营机构数字人民币钱包》] (11 May 2021) https://news.stcn.com/sd/202105/t20210511_3215489.html accessed 19 July 2026.

[13] ibid.

[14] 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 (28 June 2023).

widely used in the euro area.[15] Similar to the e-CNY, the digital euro also adopts a model that combines institutional architecture with privacy-by-design. The digital euro comprises a two-tier structure and two payment modes, online and offline, which differ in the level of privacy protection they offer.[16] About the differing levels of privacy protection under the online and offline payment models, this paper argues that although the mechanisms appear distinct, they are essentially based on the allocation of data visibility according to transaction amounts. In particular, for online payments, the digital euro adopts a level of privacy protection similar to that of current electronic payment systems.[17] In the offline payment model, commercial banks do not collect users' personal information but merely enable users to top up and withdraw the euro, with subsequent transactions being completely anonymous.[18]

1.2 Privacy Concerns within the e-CNY and the digital euro

Although the e-CNY and the digital euro differ in structure and design, the similar two-tier structure, and the visibility of data based on transaction amounts give rise to similar privacy concerns: the distribution of visibility over transaction data amongst different institutions. In particular, there are concerns regarding state surveillance resulting from central banks' access to data, as well as the potential for other private institutions to obtain excessive amounts of personal information.[19]

Firstly, the nature of these two CBDCs as central bank money enables central banks to access users' transactional data.[20] Specifically, although under the aforementioned two-tier structure it is difficult for the PBOC and the ECB to directly view all real-name transaction data, both central banks occupy a central position in currency issuance, infrastructure management and system governance, and possess the ability to access the personal information and transaction data of e-CNY and digital euro users.[21] This is made all the more evident by the e-CNY's structure, in which the central bank directly controls a unified ledger; however, even in the case of the digital euro, central banks can still utilise re-identification capabilities to track personal data. Yet, as the research by Wang Mong and Tikvah Chan has found, merely replacing real identities with ever-changing pseudonymous identifiers only

---

[15] European Commission (n 2).
[16] ibdi.
[17] ibid.
[18] ibid.
[19] Frédéric Tronnier and Weihua Qiu, 'How do privacy concerns impact actual adoption of central bank digital currency? An investigation using the e-CNY in China' (2024) 8 Quantitative Finance and Economics 126–152, doi:10.3934/QFE.2024006.
[20] Pangyue Cheng, 'Decoding the Rise of Central Bank Digital Currency in China: Designs, Problems, and Prospects' (2022) *Journal of Banking Regulation*
[21] Auer R, Frost J, Gambacorta L, et al. (2021) Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier. Ann Rev Econ.

partially resolves privacy concerns, as transaction amounts, timestamps and other relevant transaction information may still reveal details sufficient to identify or distinguish users.[22] Furthermore, as recognised in the European Commission's Proposal for a Regulation on the Establishment of the Digital Euro, the current legislative proposal merely provides that the ECB and the national central banks shall not retain personal data or transaction data relating to the use of the digital euro.[23] However, the retention of data is not the only means by which privacy may be compromised. Access to and processing of personal information alone may already constitute an interference with individual privacy, even where such data are not permanently stored.[24] Consequently, whether it be the e-CNY or the digital euro, the central bank possesses, within the structure of both systems, at least the institutional capacity to process transaction data and influence whether such data can be re-linked, thereby posing a potential threat of state surveillance.[25]

The danger of such state surveillance lies primarily in the fact that this information may be used to harm individuals. As demonstrated by Stanley I. Benn's research, the excessive collection of personal information by the government may lead to undue interference in individuals' lives, thereby diminishing their autonomy.[26] As he put it, these grievances suggest a fundamental basis for resistance: people cannot be viewed as objects or animals.[27]

Secondly, the second-tier structures of the e-CNY and the digital euro, which include intermediary operators such as commercial banks, pose a risk of excessive access to and processing of personal data. In particular, as the e-CNY and the digital euro are digital forms of legal tender, their second-tier operators currently consist primarily of designated operators such as commercial banks. These institutions are themselves classified as financial institutions under anti-money laundering legislation. Therefore, they are required to fulfil their anti-money laundering obligations.[28] For example, Article 6 of China's Anti-Money Laundering Law stipulates that established financial institutions and specific non-financial institutions required by law to fulfil anti-money laundering obligations are subject to these provisions.[29] Article 13 of EU

---

[22] Wang Mong Tikvah Chan, 'A Privacy-preserving Central Bank Ledger for Central Bank Digital Currency' (2023) arXiv:2311.16105.
[23] 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 (28 June 2023) arts 35–37.
[24] European Commission (n 2).
[25] Auer R, Böhme R (2020) The technology of retail central bank digital currency. BIS Q Rev, 85-100.
[26] Stanley I Benn, 'Privacy, Freedom, and Respect for Persons' in Richard Wasserstrom (ed), Today's Moral Problems (New York, 1975) 1, 6.
[27] ibid.
[28] Michi Kakebayashi, Gerard P Presto, Tomonori Yuyama and Shin'ichirō Matsuo, 'Policy Design of Retail Central Bank Digital Currencies: Embedding AML/CFT Compliance' (22 February 2023) 8–15.
[29] Anti-Money Laundering Law of the People's Republic of China (中华人民共和国反洗钱法) (adopted by the Standing Committee of the National People's Congress on 8 November 2024, effective 1 January 2025) art 6.

Directive (EU) 2015/849 also sets out customer due diligence measures, requiring obliged entities to identify and verify the identity of their customers.[30] Consequently, the traditional compliance obligations borne by commercial banks and other authorised institutions may pose a threat to privacy in the context of CBDCs.

Furthermore, in the digital era, personal information may be reused, posing a further threat to privacy.[31] As Marc Torrens and Amir Tabakovic have pointed out, in a data-driven society, payment data can become a key competitive advantage for private platforms, including commercial banks.[32] In the context of CBDCs, this personal information and transaction data may be used to analyse consumer preferences, thereby enabling the adoption of different marketing strategies for different customers, which poses a potential risk to privacy.[33] This is by no means an exaggeration; such practices are currently evident on major e-commerce platforms in both China and the EU. Taobao, China's leading e-commerce platform, for instance, uses consumer browsing, search and spending data to assess consumer preferences and payment capacity, and consequently offers different users varying discounts.[34] In this context, the use of users' data has effectively exceeded the scope originally promised at the time of collection, which may constitute an infringement of privacy. Furthermore, this data is currently being utilised across platforms without users' knowledge; for example, products searched for or browsed on the Taobao e-commerce platform may reappear on the TikTok platform, even though consumers have not authorised Taobao to provide their personal information and consumption data to other platforms.[35]

A similar situation exists in the European Union. In 2021, the Luxembourg Data Protection Commission imposed a fine totalling 746 million euros on Amazon, the region's leading e-commerce platform.[36] In this case, the regulatory authority confirmed that Amazon's processing of personal data in online behavioural advertising breached several provisions of the GDPR. Such online behavioural advertising typically involves monitoring consumers' browsing history, aggregating

---

[30] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73, art 13.

[31] Syngjoo Choi and others, 'Central Bank Digital Currency and Privacy: A Randomized Survey Experiment' [2022] SSRN Electronic Journal.

[32] Marc Torrens and Amir Tabakovic, 'A Banking Platform to Leverage Data Driven Marketing with Machine Learning' (2022) 24(3) *Entropy* 347.

[33] ibid.

[34] Shanshan Quan and others, 'Data-Driven Price Discrimination, Regulation, and Platform Compliance: Evidence From a Field Experiment and a Natural Experiment' (2026) Production and Operations Management.

[35] ibid.

[36] Commission nationale pour la protection des données (CNPD), 'Decision regarding Amazon Europe Core S.à r.l.' (6 August 2021).

this with their other transactional activities, predicting user preferences and, consequently, encouraging purchases.[37]

Therefore, the privacy risks associated with the use of the e-CNY and the digital euro may stem not only from state surveillance at the central bank level but also from excessive data collection by private entities. The following section will analyse the potential approaches for future legislation, starting from the perspective of how to interpret the rights involved in the privacy protection of the e-CNY and the digital euro.

II. Understanding Privacy Within the e-CNY and the Digital Euro

2.1 The Philosophical Foundation of Privacy Rights

As Julie Inness observes, the concept of privacy still exists in a chaotic world.[38] This section will analyse different perspectives of privacy and locate the essential elements of privacy rights.

Initially, intimacy is seen as the philosophical foundation of privacy.[39] Privacy rights were broadly defined as the right to be free from intrusion into one's private sphere.[40] The 'right to be let alone' theory, proposed by Samuel D Warren and Louis D Brandeis, emphasises this central role of intimacy in privacy rights.[41] Subsequently, another perspective posits that the privacy right entails limited access to one's private sphere, particularly in safeguarding against unauthorised third-party intrusion.[42] Scholars espousing this perspective further link privacy with secrecy, contending that privacy safeguards an individual's right to conceal their information, while unauthorised access or disclosure constitutes a violation of this right.[43] Under this theory, privacy constitutes a private sphere relatively insulated from external interference and surveillance, emphasising that it affords individuals 'the opportunity to experiment with self-definition in private.'[44] This concept is regarded by many scholars as a complex iteration of 'the right to be let alone'.[45]

---

[37] ibid.
[38] Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press 1992) ch 1, 4.
[39] Stanley I Benn, 'Privacy, Freedom, and Respect for Persons' in J Roland Pennock and John W Chapman (eds), Nomos XIII: Privacy (Atherton Press, New York 1971) 1.
[40] Xinyue Mei, 'Digital Transformation: The Impact of E-CNY on Securities Institutions and Financial Systems in China' (2024) 7 Proceedings of Business and Economic Studies 38.
[41] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195.
[42] María P Angel and Ryan Calo (n28).
[43] ibid.
[44] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject As Object' (2000) 52 Stan. L. Rev. 1373 at 1424. See also Elizabeth M. Schneider, "The Violence of Privacy" (1991) 23 Conn. L. Rev. 973.
[45] Richard B Bruyer, 'Privacy: A Review and Critique of the Literature' (2016) 12 Privacy Studies Journal 45.

While expressed differently, both of these theories reflect the ideas of solitude and freedom from external interference, essentially refining and elaborating upon the notion of the right to be 'let alone'.[46] In summary, privacy rights seek to preserve a private sphere free from intrusion by others and the state, with personal autonomy as their philosophical foundation. In this sense, privacy rights are primarily concerned with protecting individuals' mental tranquillity rather than preventing material harm, and are predominantly conceived as negative rights, requiring others to refrain from unjustified interference with an individual's private sphere.

2.2 The Philosophical Foundation of Personal Information Rights

With advances in computer technology, privacy concepts centred on autonomy began to reveal their limitations; it needed to analyse whether information gathering is necessary and reasonable specifically, and theories concerning the protection of personal information emerged at this stage.[47]

Against this backdrop, conceptions of personal information emerged, epitomised by Alan Westin. This phase of theory summarised personal information as our right to control information about ourselves.[48] As articulated in Alan Westin's renowned definition, 'privacy is defined as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[49] Although Westin's definition framed information control through the lens of privacy rights, it nonetheless 'provided a theoretical foundation for data protection laws across liberal democracies,' and influenced the direction of privacy policies in various countries during the 1970s.[50] Nations gradually initiated relevant legislation in the field of personal information, regulating its collection and utilisation to address the shortcomings of traditional privacy rights protection.[51]

Subsequently, Germany's Census Case established the renowned principle of informational self-determination, establishing the protection of personal information by affirming an individual's right to determine whether, when, and how their personal information is disclosed to others.[52] As articulated, 'individuals should have the right to determine how information about themselves is collected, stored, processed, and

---

[46] David Ballaschk and Jan Paulick, 'The Public, the Private and the Secret: Thoughts on Privacy in Central Bank Digital Currencies'.
[47] Darnel J. Solove, "Conceptualizing Privacy' (2002) 90 Cal. L. Rev. 1087
[48] María P Angel and Ryan Calo, 'Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy' (2024) 124 Columbia Law Review 507.
[49] Darnel J. Solove (n36) 1109-1110.
[50] Colin J Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press 1992).
[51] Weixing Shen, 'The Path of Personal Information Protection in China in the Era of Big Data' (2020) *Tan Suo Yu Zheng Ming* (Explore & Discourse) 2020(11): 5-8.
[52] Ibid.

transmitted.'[53] The informational self-determination codifies Westin's theory into a constitutional right and marks the recognition of personal information rights as an independent legal entitlement.[54] Informational self-determination has consequently become the core right principle underpinning modern data protection legislation.[55] It can be seen that privacy, centred on informational control, is understood as the ability to govern information about oneself, that is, to decide what information may be known by whom. This constitutes an active right, thereby significantly enhancing individuals' sense of control over their own information.[56]

In summary, the right to personal information control pays attention to individuals' capacity to control their own data. This stems from the identifiable and easily transferable nature of personal information; the misuse of personal information may not only intrude upon personal lives but also cause material harm through price discrimination or the trafficking of personal data. Consequently, safeguarding personal information necessitates individuals taking a more active role in controlling and directing the flow of their data.

2.3 Rights in the e-CNY and the digital euro: Privacy Rights and Personal Information Rights

Based on clarifying the philosophical foundations of privacy rights and personal information rights, this section will apply these philosophical foundations to the e-CNY and the digital euro. In this way, the paper suggests that the legal foundation for these two CBDCs' privacy encompasses both privacy rights and personal information rights.

Firstly, in transactions conducted using the e-CNY and the digital euro, although certain differences exist between the two systems, both involve the processing of transaction data in the process of account opening and the storage of transaction records. Throughout this process, users rely on privacy rights to safeguard their personal autonomy and on personal information rights to prevent unauthorised access to, processing of, or dissemination of their personal information. Accordingly, the protection of transaction data under the e-CNY and the digital euro encompasses both privacy rights, which are centred on preserving personal autonomy, and personal

---

[53] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in *Reinventing Data Protection* (Springer 2009) 45.
[54] Xinyue Mei, 'Digital Transformation: The Impact of E-CNY on Securities Institutions and Financial Systems in China' (2024) 7 Proceedings of Business and Economic Studies 38.
[55] Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89 Yale Law Journal 421.
[56] Charles Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475, 483.

information rights, which enable individuals to exercise active control over the use of their personal data.

In particular, privacy rights are intended to prevent unjustified intrusion into an individual's private sphere and the disclosure or misuse of private information, thereby safeguarding individual autonomy and psychological tranquillity.[57] For instance, in the context of e-CNY and digital euro payments, users may wish to keep their transaction details confidential in order to avoid social judgement, profiling or discrimination. Personal information rights focus on individuals' ability to control the processing of their data, including rights such as consent, withdrawal of consent and restrictions on data processing.[58] In essence, privacy rights protect users through freedom from unjustified interference, whereas personal information rights empower users by enabling them to determine how their personal data is collected, processed and used. Accordingly, transaction data privacy in the context of the e-CNY and the digital euro should be understood as encompassing both privacy rights and personal information rights, which together provide the normative basis for its legal protection.

Furthermore, as the foregoing analysis of privacy rights and personal information rights demonstrates, privacy rights are primarily concerned with protecting individuals' non-material interests, namely the autonomy to live free from unjustified interference. By contrast, personal information rights place greater emphasis on property interests, as one of the most common infringements of information control is the commercial exploitation of another person's data for economic gain.[59] Data generated through the use of the e-CNY and the digital euro embodies both personality and property interests. On the one hand, transaction data generated by these two CBDCs may reveal highly sensitive information, such as payments for legal services or healthcare.[60] In most cases, users do not wish such information to be disclosed to others. Consequently, this category of data reflects personality interests and requires protection through privacy rights. On the other hand, with the rapid development of the digital economy, particularly e-commerce, user data has increasingly become a valuable commercial asset. Businesses frequently analyse transaction data to identify consumer preferences, conduct targeted marketing, or engage in price discrimination, thereby generating additional economic value.[61] Consequently, transaction data generated through the use of the e-CNY and the digital euro also embodies significant property interests.

---

[57] Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008) 98–108.
[58] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) Yale Law Journal 421.
[59] Orla Lynskey, The Foundations of EU Data Protection Law (Oxford University Press 2015) 51–76.
[60] Daniel J Solove (n 44).
[61] Maurice E Stucke and Ariel Ezrachi, *Competition Overdose* (Harper Business 2020).

In summary, transaction data generated through the use of CBDCs embodies both personality and property interests. Consequently, it engages both privacy rights and personal information rights and requires the concurrent application of legal rules governing privacy protection and personal information protection.

III. Legal Responses to Transaction Data Protection in the e-CNY and the Digital Euro

As discussed above, transaction data protection in the e-CNY and the digital euro engages both privacy rights and personal information rights, which are grounded respectively in transactional autonomy and individuals' control over their personal information. On the basis of these normative foundations, this section develops the legal responses for the protection of each right.

3.1 Legal Protection of Privacy Rights

Regarding the protection of privacy rights in the context of the e-CNY and the digital euro, a key limitation of both the Chinese and EU legal frameworks is that they focus primarily on regulating access to transaction data, while providing insufficient regulation of the subsequent processing of such data. However, because the personal autonomy protected by privacy rights may be affected throughout the entire lifecycle of CBDC transaction data, effective legal protection should extend beyond the point of collection. Both China and the EU therefore require a more comprehensive regulatory framework governing the processing and circulation of transaction data to minimise unjustified interference with users' transactional autonomy. Drawing on Daniel J. Solove's taxonomy of privacy, this section proposes recommendations for the legal protection of transaction data within the e-CNY and the digital euro.

In China, the current data protection framework primarily consists of the Personal Information Protection Law (PIPL), the Data Security Law (DSL), and the Cybersecurity Law, which regulate personal information, data relevant to national security, and cybersecurity respectively. As this paper focuses on the use and protection of personal information in the context of the e-CNY, the following discussion concentrates on the PIPL. Article 6 establishes the principles of purpose limitation and data minimisation by requiring that personal information be processed for specific and legitimate purposes using methods that have the least impact on individual rights and interests.[62] However, these requirements primarily regulate the

[62] Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, 20 August 2021, effective 1 November 2021) art 6.

collection and initial processing of data and provide little guidance on the subsequent dissemination and secondary use of transaction data. Similarly, although Article 13 specifies the legal bases for processing personal information, it does not clearly define the limits on subsequent data use.[63]

Comparable limitations can be identified within the GDPR. Articles 5 and 6 establish the principles of lawful processing and purpose limitation, yet, in the context of the digital euro, they provide limited guidance on when transaction data may be aggregated, further analysed, re-identified or reused after lawful access has been obtained.[64] Moreover, although Article 22 protects individuals against decisions based solely on automated processing that produce legal or similarly significant effects, it does not adequately regulate less intrusive forms of data-driven decision-making, such as personalised advertising or behavioural nudging based on digital euro transaction data.[65] The purpose of this analysis is not to provide an exhaustive review of the shortcomings of either legal framework, but rather to illustrate, through representative provisions, the principal limitations of the existing legal regimes when applied to CBDC transaction data.

To address these shortcomings, this paper adopts Solove's taxonomy of privacy, which classifies privacy violations into information collection, information processing, information dissemination and invasion.[66] Since existing legislation already devotes attention to the collection of personal information, this paper argues that future legal frameworks in both China and the EU should place greater emphasis on regulating the processing, dissemination and invasion of CBDC transaction data.

Firstly, with respect to information processing, the legal authority of central banks and authorised intermediaries to process transaction data remains insufficiently defined. In practice, data processing may therefore be justified through broadly drafted authorisation provisions, such as Article 13 of the PIPL and Article 6 of the GDPR, without corresponding prohibitions limiting the scope of those authorisations. This creates the risk that transaction data will be processed based on overly broad statutory grounds.[67] Accordingly, legislation should establish clearer statutory restrictions on the categories of transaction data that may be processed by central banks and authorised institutions. Authorisations to process CBDCs transaction data

---

[63] Personal Information Protection Law of the People's Republic of China art 13.
[64] 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] OJ L119/1 art 5, art 6.
[65] Regulation (EU) 2016/679 (General Data Protection Regulation) art 22.
[66] Solove (n 49) 477.
[67] Wu Yue, 'Subduing Leviathan: Examining Central Bank Digital Currency's Privacy Protection Regime from the Chinese and European Perspectives' (2025) 33(2) Asia Pacific Law Review 207.

should be interpreted narrowly rather than expansively, so that data processing is permitted only where expressly authorised by law.

Secondly, with respect to information dissemination and invasion, stronger safeguards should be introduced to restrict both the onward transfer of transaction data and its secondary commercial use. In particular, specific rules should prohibit the disclosure of sensitive CBDC transaction data to entities whose functions are unrelated to payment services, such as marketing or insurance providers, and should prevent lawfully obtained transaction data from being reused for unrelated commercial purposes.[68] Likewise, within the GDPR framework, specific provisions governing the digital euro should further restrict the circulation and secondary use of transaction data so as to reduce the risk that such data may be exploited in ways that interfere with users' transactional autonomy.

3.2 Legal Protection of Personal Information Rights

This section draws upon Helen Nissenbaum's theory of Contextual Integrity to examine how the protection of personal information rights in the e-CNY and the digital euro can be strengthened.

Nissenbaum proposed the theory of Contextual Integrity, positing that privacy infringement should be determined by the 'appropriate flow of personal information.'[69] She identifies four parameters for determining whether information flows are appropriate: the context, the actors, the attributes of the information, and the governing transmission principles.[70] Building on this theory, this paper argues that the legitimacy and visibility of CBDC transaction data should not be determined by a single criterion, but should instead depend on the transaction context, the actors involved, the nature of the transaction data, and the applicable rules governing information flows.

Accordingly, the visibility mechanisms currently adopted by the e-CNY and the digital euro, namely controllable anonymity and the distinction between online and offline payments, should be further refined in light of these factors. In particular, different actors create different risks for individuals' control over their personal information. Where central banks process transaction data, the principal concern is the potential expansion of state surveillance. The primary risks associated with commercial banks and other authorised intermediaries lie in excessive data collection

---

[68] Ross P Buckley and others, Central Bank Digital Currency Data Use and Privacy Protection (IMF FinTech Notes No 2024/004, International Monetary Fund 2024) 18–20.
[69] Helen Nissenbaum, *Privacy as Contextual Integrity* (Stanford University Press 2010).
[70] ibid.

and the secondary commercial use of transaction data. Consequently, central banks should, generally, have no access to identifiable transaction data unless access is strictly necessary to protect specific public interests or national security. Commercial banks may retain broader access for operational purposes, but the scope and purposes of such access should be subject to strict statutory limitations.

Data visibility should take account not only of transaction value but also of the sensitivity of the transaction itself. For highly sensitive transactions, such as those involving suspected fraud, competent authorities should be permitted to authorise the re-identification of transaction data even where the transaction falls within a low-value e-CNY wallet or an offline digital euro payment, where such access is necessary to protect users' financial security. Conversely, where transaction data are of low sensitivity, such as ordinary consumer spending or routine transfers, both central banks and commercial banks should remain subject to strict restrictions on collecting and using the data, even where the transaction amount is relatively high or the payment is conducted online.

Additionally, both China and the EU should strengthen institutional safeguards through functional separation and data segregation. In the case of the e-CNY, commercial banks should establish organisational separation between departments responsible for processing the e-CNY transaction data and commercial functions such as marketing, preventing transaction data from being transferred for commercial analysis unless expressly authorised by law.[71] Within the PBOC, independent data-processing units should be established for different regulatory functions, with differentiated access permissions and a tiered approval mechanism governing the re-identification of transaction data. For the digital euro, the ECB should further clarify the allocation of data-processing responsibilities between itself and payment service providers (PSPs), ensuring that each institution may access only the transaction data necessary to perform its statutory functions and preventing transaction data from being reused for purposes unrelated to payment services, such as consumer profiling or behavioural manipulation.[72]

[71] Cheng-Yun Tsang, Yueh-Ping Yang and Ping-Kuei Chen, 'Disciplining CBDCs: Achieving the Balance between Privacy Protection and Central Bank Independence' (2023) 43 Northwestern Journal of International Law & Business 235.

[72] Mikolai Gütschow and Bernd Lucke, 'The Proposed Design of the Digital Euro: A Critical Analysis' (2026) 8 Digital Finance article 7.

Conclusion

This paper has examined how the law should respond to the tension between the degree of data visibility required for CBDCs to preserve the uniformity of central bank money and the protection of transaction data privacy. Taking China's e-CNY and the EU's digital euro as representative case studies, it has analysed the legal framework from the perspective of the fundamental rights engaged by CBDC transaction data. The analysis demonstrates that transaction data protection in the e-CNY and the digital euro cannot be understood solely through the lens of either privacy rights or personal information rights. Privacy rights are primarily concerned with protecting individuals' transactional autonomy, whereas personal information rights focus on safeguarding individuals' control over their personal data. Consequently, transaction data generated through the use of CBDCs engages both categories of rights and requires distinct legal responses. Building on this analysis, the paper argues that, from the perspective of privacy rights, future legislation in both China and the EU should place greater emphasis on regulating the processing, dissemination and invasion of transaction data after collection, rather than concentrating primarily on the collection stage. Drawing on Daniel J. Solove's taxonomy of privacy, the law should more strictly limit the processing and dissemination of transaction data in order to reduce unjustified interference with users' transactional autonomy. From the perspective of personal information rights, and informed by Helen Nissenbaum's theory of contextual integrity, the paper further argues that existing visibility mechanisms, which are largely based on transaction amounts, should be refined by taking into account the sensitivity of transaction data and the specific context in which it is used, thereby strengthening individuals' control over their personal information.