J. East Asia & Int'l L. Vol. 16/No.2 (2023); 211-232
Publication type : Research Article
Section : Issue Focus
DOI : http://dx.doi.org/10.14330/jeail.2023.16.2.01

Privacy Protection in the Context of CBDC: Development Trends and China's Practice

Xin Chen*

Central bank digital currency (CBDC) is generally defined as the digital form of a country's fiat currency. Based on the distributed ledger technology and other financial technology, CBDC could improve the efficiency of domestic and cross-border payments, increase payment safety and soundness, and promote financial inclusion. However, it is argued that the introduction of CBDC would threaten data security and invade personal privacy. Currently, this issue has received growing concern, and some recommendations are proposed by countries or international organizations, like privacy design, restrictions on public authorities and payment intermediaries, and establishing independent supervisory authority. Other suggestions include getting countries involved in international coordination and promoting the formation of unified standards. Among major economies, China is the first to launch CBDC, which is known as e-CNY. Based on an overview of the privacy protection legislation in China, this article attempts to describe the rules that should be followed when dealing with personal data generated in e-CNY circulation.

Keywords
CBDC, Privacy Protection, e-CNY, Digital Currency, Financial Technology

* Associate Professor at Xiamen University Law School, China. LL.M./Ph.D. (Xiamen U.). ORCID: http://orcid.org/0009-0003-1433-8467. The author may be contacted at: echoflying@xmu.edu.cn / Address: Law school, Xiamen University, 422 South Siming Road, Xiamen, Fujian, 361005, P.R. China.
All the websites cited in this article were last visited on November 10, 2023.

I. Introduction

There has been growing interest in the potential legal complications that may arise from the central bank's issuing of a digital currency. According to the report of the Bank for International Settlements (BIS) in May 2022, 90% of the 81 central banks who responded to the BIS questionnaire were actively engaging in CBDC research.[1] Distributed ledger technology allows for more anonymity in CBDC transactions than traditional banking or third-party payment methods. It is no secret that people prefer anonymous forms of CBDC. As a result, their financial data does not fall into the wrong hands or is subject to excessive government scrutiny. However, the administrative organ will be unable to follow the money trails of criminal activities like money laundering and terrorist financing with a CBDC that provide high anonymity. Therefore, at the outset of CBDC, striking a balance between anonymity and privacy protection is of paramount importance.

In the report of the CBDC Background Technical Note, the World Bank (IBRD) focuses on the relevance of CBDC and personal information protection, i.e. how different types of CBDC achieve anonymity.[2] The US President's Executive Order in March 2022 noted that the proliferation of digital assets (including CBDC) posed serious threats to personal data privacy and financial system integrity, so that measures should be taken to safeguard the interests of consumers, investors, and enterprises.[3] The Bank of Canada examines five forms of CBDCs, demonstrating that privacy goals must be weighed against the ease with which authorities can acquire data to satisfy legal requirements.[4] As the Bank of England has emphasized, digital pound sterling will be subject to stringent privacy protection requirements, but in order to combat financial crimes, digital pound sterling will not be fully anonymous.[5] The Bank of Japan believes that privacy protection is one of the main factors to determine whether

1 Anneke Kosse & Ilaria Mattei, *Gaining Momentum-Results of the 2021 BIS Survey on CBDC* 1 (BIS Papers No 125, 2022), https://www.bis.org/publ/bppdf/bispap125.pdf.

2 World Bank Group, Central Bank Digital Currency-Background Technical Note (Nov. 2021), at 10-3, https://documents1.worldbank.org/curated/en/603451638869243764/pdf/Central-Bank-Digital-Currency-Background-Technical-Note.pdf.

3 Executive Office of the President of the USA, Ensuring Responsible Development of Digital Assets (Mar. 9, 2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

4 Sriram Darbha, Archetypes for a Retail CBDC, Bank of Canada (Oct. 2022), https://www.bankofcanada.ca/2022/10/staff-analytical-note-2022-14/#Compliance.

5 Bank of England, HM Treasury and Bank of England Consider Plans for a Digital Pound (2023), https://www.bankofengland.co.uk/news/2023/february/hm-treasury-and-boe-consider-plans-for-a-digital-pound.

CBDC could become a widely used payment tool.[6] Therefore, the current Personal Information Protection Law and other legislation should be examined to determine whether they can provide sufficient support.[7]

As CBDC launching countries are increasing, the CBDC clearing system is estimated to become an important support for cross-border payments. However, the different privacy considerations and trade-offs in different countries/regions will create challenges or increase costs to the cross-border use and management of CBDC, and thus become a constraint on whether a country's CBDC can be widely accepted in cross-border transactions.

The primary purpose of this research is to explore the rules which should be followed in CBDC circulation, and examines whether the e-CNY system could provide adequate privacy protection while ensuring regulatory compliance and achieving public interests. This paper is composed of five parts including an Introduction and Conclusion. Part two will compare the differences in anonymity between private digital currency and CBDC, as well as an analysis of the competing legal interests. Part three will evaluate the current international experience, consensus and development trends of the applicable regulations for CBDC privacy protection. Part four will examine whether personal data generated in the circulation of e-CNY is adequately protected by the legal foundations and institutional arrangements in China, taking into account the design principles, operation models and participating organizations of e-CNY.

II. Varying Degrees of Anonymity and the Corresponding Conflicts of Legal Interests

Distributed ledger technology inspired the idea of digital currency. Tokenization, encryption and programmability are all examples of cutting-edge financial technologies that can verify a transactional authenticity and validity.[8] Digital currency can be divided into two types: private digital currency (e.g., Bitcoin, Tether) and CBDC. In September 2017, BIS proposed the famous "flower of money" model to compare the differences between private digital currency and CBDC in terms of the issuer (central

6 Bank of Japan [BoJ], Privacy Enhancing Technologies: Payments and Financial Services in a Digital Society (2023), at 1, https://www.boj.or.jp/en/research/brp/psr/data/psrb230120.pdf.

7 *Id.*

8 Tobias Adrian & Tommaso Mancini-Griffoli, Technology Behind Crypto Can Also Improve Payments, Providing a Public Good, IMF Blog (Feb. 23, 2023), https://www.imf.org/en/Blogs/Articles/2023/02/23/technology-behind-crypto-can-also-improve-payments-providing-a-public-good.

bank or commercial institution), form (tangible or electronic), accessibility (universal circulation or limited access), and verification method (intermediary intervention or decentralized).[9] The report demonstrated the similarities between the two in terms of the underlying technology and some economic functions. It further pointed out that only CBDC was issued by the central bank and had universal accessibility.[10] Therefore, the private digital currency and CBDC follow a similar technical route, adopting distributed ledger technology, smart contracts, and other encrypted digital solutions, to reduce the dependence on payment intermediaries. The corresponding legal characteristic reflects this distinction.[11] CBDC is a digital form of legal tender that serves as a guarantee with national credit, while private digital currencies are based on commercial credit.

A. The High Anonymity of Private Digital Currency

The application of distributed ledger technology endows the private digital currency with sufficient anonymity.[12] Using a public key to generate addresses, consensus algorithms to update and synchronize data, and cryptographic methods like Hash-Time Locked Contracts to secure the security of data transmission and access, the distributed ledger technology aims to overcome the trust problem in information exchange and sharing.[13] By providing records that are scattered in form but accurate in content, private digital currency does not require intermediary institutions to check transactions and verify the accuracy of records, thereby realizing the transformation from the traditional centralized organizational structure to the disintermediation model. Private digital currency transactions are not completely anonymous. However, they still leave behind traces like timestamps and IP addresses that can be used to identify and lock in the parties involved.[14]

Due to its high anonymity, private digital currency has become a conduit for a wide range of criminal acts, including the concealment and transfer of ill-gotten

9 Morten Bech & Rodney Garratt, Central Bank Cryptocurrencies (2017), at 60, https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

10 *Id*.

11 CPMI, Digital Currencies, https://www.bis.org/cpmi/publ/d137.htm.

12 Romulo Braga & Arthur Luna, *Dark Web and Bitcoin: An Analysis of the Impact of Digital Anonymate and Cryptocurrencies in the Practice of Money Laundering Crime*, 9 Direito e Desenvolvimento 271-4 (2018).

13 European Central Bank, Virtual Currency Schemes 10 (2012), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

14 Hulya Hazar, *Anonymity in Cryptocurrencies*, *in* Eurasian Economic Perspectives 171-2 (Mehmet Bilgin, Hakan Danis & Ender Demir eds., 2020).

gains, money laundering, terrorist financing.[15] At the same time, the decentralized trading mode of private digital currency makes it difficult to "know your customers," "customer due diligence," etc.[16] Because of the risk factors associated with private digital currencies, law enforcement organizations often request information from intermediate entities, such as user records or suspicious transaction reports.[17] For example, the Financial Action Task Force (FATF) added the "Travel Rule" to virtual assets, requiring countries to ensure that in the transfer of virtual assets, service providers can obtain and hold necessary and accurate records of the remitters and recipients, and provide the related data to the appropriate government agency as required.[18]

B. The Limited Anonymity of CBDC

Theoretically, CBDC can achieve high anonymity if it completely follows the technology route of private digital currency. However, legal tender is issued by the state. Due to the participation of the central bank and payment intermediaries in the operation of CBDC, CBDC has limited anonymity. They would have unprecedented access to sensitive user information. CBDC, if implemented without prudential oversight, would amplify the scope and extent of the security and privacy risks existing in today's financial transactions.[19]

CBDC can be divided into the direct mode - hybrid mode and intermediated mode - according to the degree of the central bank's participation.[20] The amount of personal information obtained by central banks and payment institutions varies across CBDC models. In the direct mode, CBDC is a person's direct claim to the central bank, which processes all payment data in real time; retains the specifics of each transaction; and maintains records of all retail CBDC assets.[21] The hybrid model includes a two-layer structure. Individuals directly request claims from the central bank. Although retail

15 Gabrielle Velkes, *International Anti-Money Laundering Regulation of Virtual Currencies and Assets*, 52(3) N.Y. U. J. Int'l L. & Pol. 876-7 (2020).

16 *Id*. at 900.

17 Sarah Hughes & Stephen Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 Yale J. Regul. 531 (2015).

18 FATF, Updated Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers (2021), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

19 Giulia Fanti, Josh Lipsky & Ole Moehr, CBDCs may Pose Security Risks, but Responsible Design can Turn Them into Opportunities, IMF (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr.

20 Raphael Auer, Giulio Cornelli & Jon Frost, *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies* 88-9 (BIS Working Papers No 880, 2020), https://www.bis.org/publ/work880.pdf.

21 *Id*.

payments are handled by intermediaries, the central bank still keeps the records of all transactions.

The original text of the BIS paper is intermediaries handle retail payments. However, the CBDC is a direct claim on the central bank, which keeps a central ledger of all transactions and operates a backup technical infrastructure.[22] Not only will direct mode and hybrid mode increase the quantity of personal information obtained by the central bank, but they will also increase the central bank's maintenance of complete transaction records pertaining to users. Obviously, it does not promote network security.

The central bank system may even become an attractive data "honeypot" for hackers. In the intermediated mode, the private sector participates in most operational business and consumer-oriented activities.[23] The central bank does not keep the record of retail transactions, but only the records of the wholesale balance of payment institutions.[24] Therefore, the central bank retains its participation in the CBDC system, only focusing on traditional mandates, e.g. releasing monetary policies and maintaining financial stabilization.[25] Because the intermediated architecture is more efficient and provides more privacy protection for end users, the intermediated mode is now favored by countries/regions that have launched or are ready to launch CBDC.[26]

As for how CBDC is generated, either token-based or account-based is an alternative. The former facilitates instantaneous, decentralized transactions between individuals via tokens. Each token has a specific par value. During the information exchange process, rather than depending on the identity of the holder, the system generates a unique digital signature to verify the transfer of the token to the payee.[27] Alternatively, account-based CBDC opens accounts at the central bank or financial intermediaries.[28] The accounts are processed by decentralized technology to avoid the information such as user identity, consumption behavior, or payment habits being

22 *Id.*

23 *Id.*

24 Raphael Auer & Rainer Böhme, The Technology of Retail Central Bank Digital Currency, BIS Q. Rev. 18 (2020), https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

25 Adina Popescu, *Cross-Border Central Bank Digital Currencies, Bank Runs and Capital Flows Volatility* 27 (IMF Working Paper No. 2022/083, 2022), https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Cross-Border-Central-Bank-Digital-Currencies-Bank-Runs-and-Capital-Flows-Volatility-517625.

26 *Id.*

27 BIS, CBDCs: An Opportunity for the Monetary System (2021), at 72, https://www.bis.org/publ/arpdf/ar2021e3.pdf.

28 Tommaso Griffoli et al., *Casting Light on Central Bank Digital Currencies* 8 (IMF Staff Discussion Notes No. 2018/008, 2018), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233.

obtained by participating entities. However, whether it is token-based or account-based, it only represents different technical solutions.[29] Personal information is still linked to actions like token generation or account creation.[30]

Accordingly, the tension between CBDC's limited anonymity and personal data protection is primarily reflected in the challenge of striking a delicate balance between the beneficial use of data and the privacy protection of the users' identities and financial details acquired by participating entities. And how to govern the public agencies like the central bank by clear rules and transparent procedures, limiting the breadth of personal data could receive through administrative management.

III. International Practice and Trends of CBDC Privacy Protection

Traditionally, privacy protection is not the goal of currency circulation. Among the existing payment methods, cash is capable of fully anonymous transactions.[31] Cash does not require an account of the central bank, as such currency issuer does not know the use and flow of cash.[32] After the emergence of bank cards and third-party payment, both domestic and cross-border transfers require the cooperation of member banks and clearing systems, and transaction records are easily captured by relevant institutions.[33] The anonymity of CBDC is between cash and bank card, as it is not completely separated from intermediaries.

Financial technology companies and payment institutions are linked by technology, which raises the risk of controlling or abusing personal data. However, as a participant in CBDC operation, the central bank should meet competition and data governance requirements, while, as a regulator to avoid systemic risk and achieve public policy objectives, the central bank should obtain necessary personal data to ensure financial stability and integrity and prevent money laundering, cyberattacks, and other illegal activities.

29 John Crawford, Lev Menand & Morgan Ricks, *FedAccounts: Digital Dollars*, 89(1) Geo. Wash. L. Rev. 151-3 (2021).

30 *Id*.

31 Alex Gladstein, *Financial Freedom and Privacy in the Post-Cash World*, 41 Cato J. 275 (2021).

32 Karin Thrasher, *The Privacy Cost of Currency*, 42(2) Mich. J. Int'l L. 403 (2021).

33 Qifan Huang, *Digitalization Reshapes the Global Financial Ecosystem* [数字化重塑全球生态], 35 Exploration & Free Views [探索与争鸣] 6 (2019).

A. International Discussion on CBDC Privacy Protection

Neither authorities nor market participants can foresee the potential dangers to privacy and the significance of privacy protection at the peak time of cash use. Electronic payment mechanisms have clearly evolved in a different direction from the complete anonymity of cash society, with private firms performing identity processes and administering consumer accounts.[34] After the cash was gradually replaced by electronic payment, fewer payment options could provide higher anonymity. Sometimes, electronic payment service providers even implement price discrimination through the use of algorithms to distinguish consumers' data.[35]

In August 2018, the UN Human Rights Council released "The Right to Privacy in the Digital Age," which clarified the basic principles, standards, and best practices for promoting and protecting the right to privacy in the digital age.[36] The report emphasizes that as the consumer digital footprint continues to grow larger, states and businesses increasingly rely on personal data, and the state has the responsibility to protect privacy.[37] In the digital era, this is also applicable to CBDC.

The CBDC reports of the international organizations and central banks have repeatedly mentioned the trade-off between privacy protection and the goals of financial stability, monetary policy, financial inclusion, and the efficiency and security of payment system. BIS emphasizes that privacy protection does not require complete anonymity.[38] The Bank of Singapore analyzed the different goals of CBDC, suggesting that growing desire of the public for privacy protection be weighed against the data monitoring needed by law enforcement.[39] According to the European Central Bank, complete anonymity will raise concerns that the digital euro will be possibly used for illegal purposes.[40] It can be concluded that anonymity is not the only goal of issuing CBDC, but should strike a balance between privacy protection and public interests.

34 Ellie Rennie & Stacey Steele, *Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency*, 3(1) L. Tech. & Hum. 7 (2021).

35 Michal Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30(2) Harv. J. L. & Tech. 331-2 (2017).

36 HRC, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31, at 2, https://undocs.org/en/A/HRC/39/29.

37 *Id.*

38 Raphael Auer et al., *Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier* 14 (BIS Working Papers No. 976, 2021), https://www.bis.org/publ/work976.pdf.

39 Monetary Authority of Singapore, A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context (2021), at 29, https://www.mas.gov.sg/-/media/MAS/EPG/Monographs-or-Information-Paper/A-retail-CBDC---Economic-Considerations-in-the-Singapore-Context.pdf.

40 ECB, A Digital Euro that Serves the Needs of the Public: Striking the Right Balance, Introductory Statement by Fabio Panetta, Member of the Executive Board of the ECB (Mar. 30, 2022), https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.en.html.

B. Suggestions for Privacy Protection in the Context of CBDC

In recent years, several recommendations and guidelines were introduced for protecting privacy during the discussion of CBDC from international organizations. The Group of Seven (G7), for instance, released its Public Policy Principles for retail CBDCs (hereinafter the Principles) in October 2021.[41] The third item of the Principles is "data privacy," which points out that strict privacy standards, the responsibility to protect user data and information transparency are essential elements for CBDC to gain trust.[42]

Legitimacy, purpose limitation, data minimization, transparency and accountability, and user consent are all fundamental tenets for the collection, storage and disposal of personal information.[43] The 2021 Annual Report of the UN on the Right to Privacy in the Digital Age proposes that an independent data privacy monitoring agency is a key element to coping with the increasingly complex and opaque global data environment (including its huge information asymmetry).[44] The development of laws on privacy protection is still up for debate because most nations outside the Bahamas and the Eastern Caribbean Monetary Union have not yet launched CBDC. Therefore, this section mainly discusses the impact of the existing rules of various countries on privacy and personal information protection as well as of safeguarding sensitive data by separating out various information processing scenarios.

1. Privacy Design of CBDC

In the realm of data compliance, the phrase "protect privacy from the beginning of design" carries a great deal of weight. Incorporating privacy design principle is integral to how they carry on business. This principle is also reflected in the reports of international organizations and the domestic legislation in multiple countries/regions. The UN recommended that governments adopt safeguards related to digital identity when realizing their full utility of data.[45] It is also contained in the Data Protection Directive in 1995 and the General Data Protection Regulation (GDPR) in 2016.[46] In addition, the Bank of Canada, comparing different privacy technologies like

41 G7, Public Policy Principles for Retail CBDCs (2021), at 1-27, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf.

42 *Id*. at 7.

43 *Id*.

44 HRC, *supra* note 36.

45 Report of the Secretary General, Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation, U.N. Doc. A/74/821, https://digitallibrary.un.org/record/3864685.

46 The Data Protection Directive 1995, pmbl. 46; The General Data Protection Regulation 2016, recital 78 & art. 25.

group signature, secret sharing, zero-knowledge proof, homomorphic encryption, multi-party computation, etc., suggested that verification efficiency and computing power be the deciding factors when choosing a particular method.[47] As proposed by the European Central Bank, "anonymous vouchers" would allow users to transact digital currency without revealing their identities or transaction histories to the central bank or intermediary institutions.[48]

Furthermore, in the joint research project Stella, the European Central Bank and the Bank of Japan attempted to isolate the payment and collection information of individual users, hide transaction details, and create "noise" in the data exchange between users and financial institutions so as to reduce the possibility of connecting relevant transaction information with individuals.[49]

The Bahamas was the first country in the world to issue CBDC. Among the Sand Dollar Wallets coming in three different varieties, the basic wallet can be opened without identity certificate. It is used for accounts with low net value, whose account balance is no more than 500 sand dollars and the monthly transaction volume is less than 1500 sand dollars.[50] Concurrently, Sand Dollar implements privacy-enhancing technologies like using encryption, assigning unique passwords for customers, and installing hardware or software suited to varying degrees of security risk.[51] As a result, the core of privacy design is an active prevention rather than passive relief, and the technology to enhance privacy protection (such as coding, pseudonym and encryption) is embedded in the CBDC scheme in advance.

2. Restrictions on Public Authority

In the conventional bankcard-based payment system, the confidentiality duty of financial institutions lies in the heart of the restrictions on the handling of personal financial information. For example, the US's Bank Secrecy Act of 1970 permits financial institutions to keep records of customers' transactions (deposits and withdrawals, transfers, etc.) and urges them to disclose to law enforcement agencies in accordance

47 Sriran Darbha & Rakesh Arora, Privacy in CBDC Technology, Bank of Canada (June, 2020), https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9.

48 ECB, Exploring Anonymity in Central Bank Digital Currencies (2019), at 1, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785.

49 ECB & BoJ, Balancing Confidentiality and Auditability in a Distributed Ledger Environment (2020), at 5, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf.

50 Central Bank of the Bahamas, Consumer-Centric Aspects of the Proposed Regulations for the Bahamian Digital Currency (Mar. 26, 2021), at 4-5, https://www.centralbankbahamas.com/viewPDF/documents/2021-03-26-12-00-35-PSD-Policy-Paper-on-Consumers-Issues.pdf.

51 *Id.*

with procedures of criminal investigation.[52] However, this disclosure often conflicts with the confidentiality obligations of financial institutions.

As a result, the Financial Privacy Rights Act regulates how and under what circumstances financial institutions should share customers' financial details with the federal departments.[53] Then, the US restrictions on public authorities were tightened in 2016 with the formation of the Federal Privacy Commission. In the EU, processing "necessary for the performance of a task carried out in the public interests or in the exercise of official authority vested in the controller" is explicitly recognized under the GDPR.[54] The right to personal privacy is also included in the EU Fifth Money Laundering Directive (2018/843),[55] because preserving public order and preventing criminal acts like money laundering are interconnected goals.

After the release of Sand Dollars in the Bahamas, the country's central bank does not participate in front-end customer service, although it does keep track of all its constituent digital currency ledgers.[56] Although the central bank of Bahamas requires digital wallet service providers to provide relevant information, it is limited to inclusive financial and statistical economic data based on the needs of public interests.[57] Therefore, despite the fact that CBDC prioritizes privacy protection, it must nevertheless achieve other policy objectives like tax management, anti-money laundering/counter-financing of terrorism (AML/CFT), etc. For the sake of transparency and accountability, it is important that the applicable legislation make clear the particular conditions under which the administrative organ handles CBDC's personal information. This will guarantee that any deviation from the right to privacy is justified by legal requirements.

3. Restrictions on Payment Institution

The US takes an industry-by-industry approach to regulate the handling of personal information by payment institutions. Payment services, which fall under the "financial services," have been associated with financial consumer protection.[58] The Federal Trade Commission is a specialized agency responsible for the protection of

52 31 U.S.C. § 5311.

53 Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22.

54 The General Data Protection Regulation 2016, art. 6.1(e).

55 EU Directive 2018/843 of the European Parliament and of the Council, ¶ 28.

56 Central Bank of the Bahamas, *supra* note 50.

57 *Id.*

58 Joseph Dehner, *The United States' Perspective on Data Protection in Financial Technology (Fintech), Insurance, and Medical Services*, 44(1) N. Ky. L. Rev. 13-4 (2017).

consumers (including financial consumers).[59] Chapter 16 of the United States Code of Federal Regulations defines financial information as "identifiable non-public personal information generated by individuals in the process of consumption or service by financial institutions."[60] It further requires financial institutions to "respect customer privacy; protect the security and confidentiality of customer's non-public personal information"; and prohibit the disclosure of such information to independent third parties, unless the customer grants the right or other exceptions apply.[61]

Different from the piecemeal legislation in the US, the EU adopts an omnibus legislation model.[62] Also, the EU considers privacy-based protection of personal data to be a fundamental right.[63] Therefore, between the free flow of information and the protection of rights, the value of the latter is given priority.[64] GDPR specifies "personal data," particularly describing "genetic data," "biological identification data," and "health-related data." However, it does not regard financial information as a special type.[65] Meanwhile, the EU does not adopt "financial institutions" to define the entity providing financial services, but defines data controllers, processors, and third parties.[66] Data controllers need to have valid grounds for processing personal data, such as by a clear affirmative consent, compliance with a legal duty.[67]

In the Bahamas, the management of electronic payment has been established before the issuance of sand dollar. The Payment System Law of 2012 and the Regulations on the Supervision of Payment Instruments of 2017 both imposed requirements like notification and consent, requirements for consumer protection, and Internet security. These suggestions were reaffirmed in the 2021 Bahamas Regulations on the Administration of Digital Currency.[68] Article 11 of the Regulations on the Administration of Digital Currency (record keeping, reporting and security audit) stipulates that digital wallet providers should take appropriate measures to protect

59 *Id.*

60 United States Code of Federal Regulations, ch.16, §313. It states about consumer financial privacy information rules.

61 *E.g.*, If there are credible evidence of individuals or entities engaging in terrorist or money laundering acts, the Patriot Act mandates financial institutions to share information with regulatory authorities or law enforcement authorities. *See* the Patriot Act 2001, § 314.

62 Bo Zhao & Weiquan Chen, *Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China*, 16(3) USA-China L. Rev. 98 (2019).

63 *Id.* at 97.

64 Haile Zhao, *Personal Information Protection from the Perspective of Data Sovereignty: International Legal Conflicts and Countermeasures* [数据主权视角下的个人信息保护国际法治冲突与对策], 36 Contemp. L. Rev. [当代法学] 85-7 (2022).

65 The General Data Protection Regulation 2016, arts. 4.13 & 4.14.

66 *Id.* arts. 4.7, 4.8 & 4.10.

67 *Id.* arts. 4.11 & 5.1.

68 Central Bank of the Bahamas, *supra* note 50.

customers from unauthorized data access by third parties.[69] It can be concluded that the principle of informed consent is universally recognized as a procedure that places limits on data processors dealing with personal data. In most cases, however, even "full disclosure and independent consent" only means that the data entity knows that personal data is processed, but not means the data entity has fully measured the risks. Therefore, the legality, validity, and necessity principles must be reviewed in the course of CBDC personal data processing.

4. Independent Supervisory Authority

The data privacy protection system regulates the administrative organs and commercial institutions when they are processing personal data. If the same administrative organ is responsible for the supervision of the industry, there will be overlapped between the regulator and the regulated.[70] In this respect, the EU put the priority on the autonomy of the specialized agencies. The independence of the national personal information protection authorities is important when judging whether overseas countries have the adequate personal data protection and could transfer domestic personal data to overseas countries. GDPR mandates that member states set up external bodies to monitor compliance and enjoy independent guarantees in terms of personnel employment, employee performance, capital budget, etc.[71]

Similar to the EU, in the Latin American and Caribbean region, Ecuador has established a data protection agency, which is an independent public institution. Nicaragua established the Personal Data Protection Bureau within the Ministry of Finance and Public Credit, which is responsible for reviewing the use of public and private data. Also, Uruguay has set up the Personal Data Supervision Bureau, which is a decentralized organization of the government.[72] Therefore, the majority of nations have adopted the manner in which independent agencies exercise their supervisory powers in accordance with the law to avoid external or internal, direct or indirect influence, and have granted them administrative powers including punishment, order, and prohibition, as well as flexible powers including education, advice, and suggestion.

69 *Id.*

70 Tao Zhang, *Organizational Law Structure of Independent Regulators in Personal Information Protection*, 40 Hebei L. Sci. 104 (2022).

71 The General Data Protection Regulation 2016, arts. 51 & 52.

72 HRC, Privacy and Personal Data Protection in Ibero-America: A Step towards Globalization?, U.N. Doc. A/HRC/49/55 (Mar. 23, 2022), https://www.ohchr.org/en/documents/thematic-reports/ahrc4955privacy-and-personal-data-protection-ibero-america-step-towards.

C. International Coordination and Cooperation

The legislation of a country or region has an effect on other jurisdictions. The adequacy requirements of GDPR for the cross-border flow of data is a typical example. In order to guarantee the cross-border payments of CBDC, international coordination and cooperation are indispensable.[73] The World Economic Forum points out that privacy and personal information protection will be the key areas of cross-border CBDC conflict in the future.[74] The East Caribbean Monetary Union, which has issued CBDC, consists of eight nations. The Union promises that all procedures for processing data in D-Cash will comply with the GDPR and international standards, as well as national legislations.[75]

Interoperability across international CBDC systems is also under consideration by various central banks.[76][77] For instance, the technology company R3 utilizes both Corda and Quorum, two different distributed ledger systems, in the Dunbar project. They adopts and constantly improves the interoperability between different privacy enhancement technologies.[78] Standards are also an integral part of interoperability.[79] Coordinating the multinational CBDC system's conformity with a unified privacy enhancement standard can win over the largest number of countries' support. The International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) are both international institutions which formulate international internet standards. In its report, the ITU's Focus Group on Digital Currency (which includes digital fiat currencies) identifies privacy and consumer protection as areas in urgent need of standardization.[80] In February 2023, ITU Working Group 17 (Security) jointly initiated a discussion with ISO/TC/307 Working Group on "Security, Identity

73 ITU Financial Inclusion Workstream, Policy and Governance Working Group, "Digital Currency Global Initiative (2022), at 4, https://www.itu.int/en/ITU-T/extcoop/dcgi/Documents/Final%20Report_DCGI_Digital%20Currencies%20and%20Financial%20Inclusion.pdf.

74 Sheila Warren et al., Digital Currency Governance Consortium White Paper Series (2021), at 33, https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf.

75 ECCB, DCash-Frequently Asked Questions, https://www.dcashec.com/faqs/security.

76 BIS, Central Bank Digital Currencies: System Design and Interoperability (2021), https://www.bis.org/publ/othp42_system_design.pdf.

77 BIS, Innovation Hub Work on CBDC, https://www.bis.org/about/bisih/topics/cbdc.htm.

78 BIS, Project Dunbar, International Settlements Using Multi-CBDCs (2022), https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm.

79 BIS, *supra* note 76.

80 International Telecommunication Union [ITU], Focus Group Digital Currency including Digital Fiat Currency: Regulatory Challenges and Risks for CBDC (2019), at 13, https://www.itu.int/en/ITU-T/focusgroups/dfc/Documents/DFC-O-006_Report%20on%20Regulatory%20Challenges%20and%20Risks%20for%20Central%20Bank%20Digital%20Currency.pdf.

Management, and Privacy of Distributed Ledger Technology."[81]

To sum up, discussions about CBDC in different nations address such issues like limited anonymity, reasonable use of personal data by payment intermediaries and rigorous restriction on the public authorities. CBDC will not function well with too much bias in either direction. The technical design, reliable data governance and personal information protection framework of CBDC will enhance the public trust and encourage them to use CBDC. Public authorities in the CBDC system should only process personal data to the extent necessary for fulfilling their statutory tasks and other lawful purposes. The private sector shall access, hold or process personal information based on agreement. Personal data shared beyond the scope of basic needs must have explicit consent and this data process should have clear reason.

IV. Privacy Protection of e-CNY in China

When it comes to CBDC, China continues to be ahead of the curve both in financial innovation and payment infrastructure.[82] By December 2022, China's e-CNY pilot had expanded to 17 provinces and cities, covering wholesale and retail, catering, culture and tourism, public services and other online and offline fields.[83] Both traditional commercial banks and private banks using high-tech like Mybank and Webank are among the e-CNY operating institutions.[84] In October 2020, the People's Bank of China issued a revised draft of the Law of the People's Bank of China, clarifying that "RMB includes both physical and digital forms."[85] The official White Paper of E-CNY, published in July 2021, considered it as the digital form of legal tender, emphasizing that e-CNY is a cash alternative which may be used to settle public and private debts.[86]

81 ITU, Meeting in Focus-Joint ITU-T SG17/ISO TC 307 Workshop on "DLT Security, Identity Management and Privacy," https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx.

82 Heng Wang, *China's Approach to Central Bank Digital Currency: Selectively Reshaping International Financial Order?*, 18(1) U. Pa. Asian L. Rev. 106 (2022).

83 Shi Jing, *Digital Yuan Continues Domestic March*, China Daily (Dec. 27, 2022), http://www.chinadaily.com.cn/a/202212/27/WS63aa2668a31057c47eba6406.html.

84 Li Bing, *E-CNY Stimulates Consumption and Licensed Consumer Finance Institutions 'Run into the Market* [数字人民币探索应用亮点纷呈，成普惠金融"助推器"], Sec. Times [证券时报] (Dec. 15, 2022), at A3.

85 Law of the People's Bank of China, art. 19.

86 People's Bank of China, Progress of Research & Development of E-CNY in China (2021), at 5, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.

A. The Necessity of Privacy Protection: Reducing Criticism on "Digital Authoritarianism"

Under the CBDC system, the central bank not only issues money, but also takes part in its operation and circulation including the access to personal data.[87] It is assumed that China may utilize the CBDC system as a new tool for social control.[88] The "digital authoritarianism" asserts that China's development of digital technology does not follow a market-oriented economy model, but instead place an emphasis on the country's dominant position and engages in excessive monitoring abroad by means of foreign exchanges.[89] In January 2021, the New National Security Center (CNAS) issued a research report, urging the US State Council to request China to publicly explain the collection and management of data on e-CNY users, so as to prevent the Chinese government from expanding its authority with the flow of natural persons or business transactions across the border.[90] In June 2021, President Biden signed an executive order, reiterating that Apps developed or controlled by China collect a large number of personal information of American individuals, damaging the national security, foreign policy and economic interests of the US. In this respect, the US government should evaluate the foreign software and set up identification standards to filter out Apps that pose unacceptable risks.[91]

The US considers the Sino-US relationship as a contest between the two distinct political and economic system.[92] The US is concerned that the internationalization of CNY "dramatically affect global finance and political-economic governance with transformative implications."[93] China primarily aims to enhance strategic alignment in the field of financial architecture with other countries for its economic growth.[94] For

87 Kimberly Houser & Colleen Baker, *Sovereign Digital Currencies: Parachute Pants or the Continuing Evolution of Money*,18(2) N.Y. U. J. L & Bus. 574 (2022).

88 Jake Laband, *Existential Threat or Digital Yawn: Evaluating China's Central Bank Digital Currency*, 63 Harv. Int'l L. J. 520 (2022).

89 Guozhu Liu, *Digital Authoritarianism' Theory and the Major Power Competition in the Digital Age* ["数字威权主义"论与数字时代的大国竞争], 36 Am. Stud. Q. [美国研究] 41 (2022).

90 Yaya Fanusie & Emily Jin, China's Digital Currency: Adding Financial Data to Digital Authoritarianism (2021), at 1, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Chinas-Digital-Currency-Jan-2021-final.pdf?mtime=20210125173901&focal=none.

91 The White House, Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries (June 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries.

92 Shen Wei & Joel Slawotsky, *Renminbi-Centric Global Financial System: China's Statecraft and Multi-Polarity*, 51(1) H.K. L. J. 765 (2021).

93 Joel Slawotsky, *US Financial Hegemony: The Digital Yuan and Risks of Dollar De-Weaponization*, 44(1) Fordham Int'l L. J. 40 (2020).

94 *Id.*

this goal, the PRC government should strike a balance between privacy right and the legitimate operation of e-CNY.[95] Mu Changchun, the director of the Digital Currency Research Institute of China pointed out that "protection of user privacy in e-CNY is of the highest level among existing payment instruments."[96] In this regard, China should participate in correlated discussions of the international financial organizations such as the IMF, BIS, G20, and FATF to avoid the arbitrary assertion. Public entities and market actors should actively participate in ITU and ISO's formulation of international privacy protection standards. In response to the potential risk of privacy erosion posed by the e-CNY, China should employ stringent privacy design and actively address international concerns regarding the protection of personal privacy in China.

B. Privacy Design of e-CNY

Regarding its mode of operation, e-CNY utilizes a two-tiered system such as commercial banks and third-party payment institutions responsible for its circulation.[97] The People's Bank of China is responsible for the interconnection and administration of e-CNY wallets among the participating institutions. In the design of privacy protection, e-CNY adopts the principle of "anonymity for small value and traceability for high value."[98] e-CNY is transported in a digital wallet, which can be either a soft wallet stored in and App or hard wallet with a physical existence.[99] e-CNY APP shows that digital wallets are categorized by the amount in the account. The fourth type of wallets could be opened by a mobile phone number whose maximum single payment is no more than CNY 2000. Given e-CNY wallets are processed using a pseudonym mechanism, the People's Bank of China only processes inter-institutional transaction information transferred through the e-CNY system.[100] Regarding the data generated by the wallet service, the participating institutions should adhere to the customer information protection rules and establish an internal control management mechanism.[101] Consequently, by following the privacy design principle, data

95 Hatim Hussain, *Central Bank Digital Currencies: Reinforcing Public Trust*, 14 Amster. L. F. J. 29 (2022).

96 China Finance 40 Forum, Will Digital RMB Violate Privacy?, Speech by MU Changchun, Director of the Digital Currency Research Institute of the People's Bank of China, http://new.cf40.org.cn/uploads/202104mcc.pdf.

97 The People's Bank of China, *supra* note 86.

98 Tianyuan Zhang, *Digital Yuan Strikes Balance on Privacy*, China Daily (Nov. 18, 2022), http://www.chinadaily.com.cn/a/202211/18/WS63772125a31049175432a90e.html.

99 Qiuyu Wu, *E-CNY Impulses High Quality Development* [数字人民币，为高质量发展添动力], People's Daily [人民日报] (July 20, 2022), at 6.

100 Changchun Mu, *The Balance between Privacy and Security: Theoretical Research and Practical Exploration of Controlled Anonymity in E-CNY* [改革创新」穆长春：隐私与安全的平衡之道-数字人民币可控匿名的理论研究与实践探索长安街读书会关注], Paper (Aug. 31, 2022), https://www.thepaper.cn/newsDetail_forward_19701039.

101 *Id.*

processors in the circulation of e-CNY satisfy their data protection responsibilities when developing, designing and selecting applications to complete their duties.

C. Rules for Privacy Protection

Even if the same information is possessed by different processors, the interests involved are distinct.[102] Based on the authorization or content from the users, commercial banks and third-party payment institutions acquire user data; provide services; and realize their commercial interests in the operation of e-CNY. Besides payment institutions, central banks and technology providers also obtain various types of personal data and realize public and commercial interests by exploring the information value. Currently, China's Civil Code and Personal Information Protection Law regulate the collection, storing and transmission of customer information, obligations of processors, privacy rights of individuals and legal accountability procedures.[103]

1. Scope of Personal Data in e-CNY

Personal data in the context of e-CNY are mainly financial information. They are, for example, the information obtained by the central bank, designated operational institutions, and counterparties in the course of providing services, that can identify an individual's identity, property or other economic features. The Civil Code lists the types of personal information which are "public information recorded by electronic or other means. It can identify specific natural persons individually or in combination with other information."[104] Article 4 of the PRC Law on Personal Information Protection stipulates a similar definition, but emphasizes on the connection to specific individuals. Concurrently, "financial accounts" are specifically defined in Article 28 of the PRC Personal Information Protection Law as an example of sensitive information.

Conversely, financial sector departmental regulations of China such as the Notice on the Protection of Personal Financial Information by Banking Financial Institutions (2011), the Regulations on the Administration of Credit Investigation (2013), and the Implementation Measures for the Protection of the Rights and Interests of Financial Consumers (2016) (hereinafter the Measures), clearly define the scope of financial information. For instance, the Measures define financial information as identity, property, account, credit, financial transactions and other information obtained,

102 Lijie Wang, *Construction of the Review Standard System for the Principle of Proportionality in the Processing of Personal Information* [个人信息处理中比例原则审查基准体系的建构], 4 L. Sci. [法学] 50 (2022).

103 The Civil Code of the People Republic of China, arts. 1034-37; The Personal Information Protection Law of China, ch. 2.

104 The Civil Code of the People Republic of China, art. 1034.

processed and stored by financial institutions through business or other channels.[105]

However, not every data is equally sensitive. For example, the sensitivity of account opening time and opening institution is lower than that of payment transaction password or personal biometric information. Therefore, when defining the scope of e-CNY personal data, the Personal Financial Information Protection Technical Specification (2020) could be used for reference. Separate kinds of personal data are identified and managed in a hierarchical fashion based on the degree to which disclosure could compromise the data subject's physical or financial safety.[106]

2. Rules for Public Authority

In China, the Personal Information Protection Law follows a "unified legislation" model, i.e., both private institutions and government agencies apply the same legislation.[107] Then, considering the differences between these two entities, special provisions are provided for the public authority. The phrase "necessary for performing legal duties [为履行法定职责所必须] is cited as the justification for the handling of personal information by administrative authorities. Cases of money laundering and tele-fraud with e-CNY were recorded in a number of locations across China in 2021-22, including Xinmi City in Henan Province, Gaoyou City in Jiangsu Province, Teng County in Guangxi Province, Nanjing in Jiangsu Province, and others.[108] Therefore, anti-fraud, AML/CFT and the protection of personal property security are the legal grounds for administrative organs to handle personal data.

In addition, personal data has a significant social and public dimension in the context of administration and services supplied by public authorities. The Law of the People's Bank of China stipulates the responsibilities of the central bank, such as "issuing and managing the circulation of RMB; foreign exchange management; maintaining the normal operation of the payment and clearing system; and taking charge of the fund monitoring of anti-money laundering."[109] Instead of viewing "safeguarding public interests" as an overarching goal, this article are concretized by listing the administrative tasks of the central bank.

Also, the relevance between the performance of legal duties and the processing

105 The Implementation Measures for the Protection of the Rights and Interests of Financial Consumers art. 27.

106 The Personal Financial Information Protection Technical Specification, art. 4.2.

107 Yikun Wang, *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], 42(6) China L. Rev. [中国法律评论] 210 (2021).

108 Fucai Ma, *The First Case of Using E-CNY to Launder Money was Solved* [《国内首例利用数字人民币洗钱案告破》], Democracy & L. Times (Nov. 25, 2021), at 3; Jing Zhu, *New Scam: Beware of the Fraud Traps behind e-CNY*, Jingling Evening News (Dec. 11, 2022), at 4.

109 The Law of the People's Bank of China, art. 4.

of personal data is described by Article 1036 of the Civil Code, which states that "in order to safeguard the public interests or the lawful rights and interests of the natural person." Moreover, Article 34 of the Personal Information Protection Law states that it "shall not exceed the scope and limits necessary for the fulfillment of their statutory functions." In this respect, capital control, promoting the balance of international payments and maintaining financial stability are all examples of the goals served by foreign exchange management. As a result, the State Administration of Foreign Exchange should supervise the transfer of funds between nations using e-CNY. However, whether e-CNY is used abroad for shopping, tourism or catering consumption, is not necessarily related to foreign exchange management and does not belong to the scope of "necessary."

3. Rules for Payment Institution

In China, rules for protecting financial information processed by payment institutions are based on two foundations: (1) the traditional obligation to keep customer data confidential; and (2) the protection of critical data to maintain network security. The traditional obligation of confidentiality of financial information originated in the era of "small data." In this regard, the purpose of utilizing customer data is for identity recognition. Given the ever-changing digital age, however, the continuous circulation of data is an inevitable trend for the growth of the financial sector. The Personal Information Protection Law and the Implementation Measures for the Protection of the Rights and Interests of Financial Consumers begin to extend from traditional static protection to the compliant use of personal financial information during the data flowing process.

First, due to the processing of sensitive personal information such as financial accounts, its constraints are more stringent which is easily triggering legal mechanisms. The Personal Information Protection Law requires that the processing of sensitive personal information be based on the principle of general prohibition and its processing have a specific purpose and sufficient necessity.[110] Sensitive personal information processing activities shall comply with the special restrictions of other laws and administrative regulations.[111]

Second, the Implementation Measures for the Protection of the Rights and Interests of Financial Consumers outlines the rules to be followed to ensure the protection of financial information provided by consumers, as well as the guidelines to be observed

110 The Personal Information Protection Law 2021, art. 32.

111 *Id.* art. 28.

when gathering sensitive information.[112] It also requires financial institutions not to use the personal financial information unrelated to financial products or services in the form of general authorization.[113] This regulatory framework provides positive incentives and reserve restraints for financial markets and market entities in order to respond to the varied values of financial information in the digital age.

4. Independent Supervisory Authority

As a central coordination agency, the Cyberspace Administration of China is responsible for regulatory oversight and enforcement of relevant law. However, it is not the single specialized supervision organization.[114] As an illustration, the People's Bank of China exercises its supervisory authority in the financial sector when commercial banks and payment institutions fail to fulfill their obligations to secure consumer financial information.[115] As mentioned earlier, the People's Bank of China may obtain personal information in e-CNY. In this case, however, there is still a risk of improper disclosure, abuse, and even theft. Actually, the People's Bank of China has the administrative power to issue and manage e-CNY and to secure financial information.

To avoid potential conflicts of interest, therefore, the Cyberspace Administration as the exclusive, independent personal data protection authority, should aid in strengthening overall process oversight and inspection and provide guidelines for evaluating privacy protection under specific scenarios. If payment intermediaries violate laws or administrative regulations, the Cyberspace Administration may take administrative penalties such as warning, ordering correction, confiscating illegal income or fines, and revoking business licenses or marketing licenses.[116] It also has the power to issue correction orders to administrative authorities such like the People's Bank of China, if these authorities violate their duty to protect personal data privacy, which will face legal consequences.[117]

112 The Implementation Measures for the Protection of the Rights and Interests of Financial Consumers, ch. 3.

113 The Cybersecurity Law art. 41; The Implementation Measures for the Protection of the Rights and Interests of Financial Consumers, arts. 29 & 30.

114 The Personal Information Protection Law 2021, art. 60.

115 The Implementation Measures for the Protection of the Rights and Interests of Financial Consumers, art. 5.

116 The Personal Information Protection Law 2021, art. 66.

117 *Id*. art. 68.

V. Conclusion

The key elements of personal data protection system include data subjects' rights, data processors' obligations, and a specialized oversight organization. First, the e-CNY system relies heavily on privacy design, which ought to be followed in the e-CNY releasing and operating procedure. Second, in order to limit the inappropriate uses of personal data collected through the e-CNY operation, it is important to categorize the data according to its sensitivity, and then build a hierarchical regulating system. Thirdly, the independent and specialized authority's unbiased supervision can increase public confidence in the security of personal data. Finally, strict civil, administrative, and criminal liability should be imposed for the improper disclosure or misuse of the data generated in the circulation of e-CNY.

Internationally, unequal personal data handling in different countries/regions can lead to the fragmentation of cross-border clearing networks; increase the compliance costs of market participants; and reduce the efficiency of payments. In practice, rules have practical effect not just when backed by official authority (like legislation or mandated standards), but also when driven by pragmatic considerations or market pressure (like voluntary standards). Regarding the cross-border flow of e-CNY, the clearing infrastructure should be interoperable to achieve financial inclusion and to facilitate the individuals and businesses to engage in transactions across jurisdictions. In conclusion, China has to be more involved in international coordination and the creation of standards, to dispel fears of "digital authoritarianism" abroad and to courage the internationalization of CNY.

Received: August 1, 2023
Modified: September 15, 2023
Accepted: November 1, 2023