The Digital Euro and Privacy in the EU: An Evaluation of Legal, Technical, and Economic Trade-Offs

By

Alberta Bikaj

Submitted to
Central European University
Department of Economics and Business

In partial fulfilment of the requirements for the degree of Master of Arts Economic Policy in Global Markets

Supervisor: Tomy Lee

Vienna, Austria
10th June 2025

COPYRIGHT NOTICE

For bibliographic and reference purposes, this thesis should be cited as:

Bikaj, A. (2025). *The Digital Euro and Privacy in the EU: An Evaluation of Legal, Technical, and Economic Trade-Offs*. MA thesis, Department of Economics, Central European University, Vienna.

AUTHOR'S DECLARATION

I, ***Alberta Bikaj***, the undersigned candidate for the MA/MSc degree in ***Economic Policy in Global Markets*** declare herewith that the present thesis titled ***The Digital Euro and Privacy in the EU: An Evaluation of Legal, Technical, and Economic Trade-Offs*** is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography.

I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Vienna, on **10.06.2025** Full Name: Alberta Bikaj

Abstract

This thesis evaluates whether the European Central Bank's proposed digital euro can offer meaningful privacy within the boundaries of EU regulation. As digital payments grow and cash usage declines, privacy in payment systems becomes more economically and politically relevant. In the EU context, this intersects with strong legal standards, including the General Data Protection Regulation, the ePrivacy Directive, anti-money laundering rules, and the Markets in Crypto-Assets Regulation. The research questions if meaningful privacy can be met by both regulatory requirements and user expectations. The analysis takes a comparative and interdisciplinary approach, drawing on regulatory texts, policy documents, technical papers, as well as global CBDC case studies.

The findings suggest that the current design provides limited privacy and relies on institutional choices rather than hard guarantees. While some privacy features are included, their scope is constrained by legal, technical, and economic trade-offs. Case studies indicate that privacy preserving CBDC models are feasible but require clearer prioritization of tradeoffs. The thesis concludes that privacy remains a core feature of trust in public money and should be considered an integral component of the digital euro's design.

Keywords: CBDC, digital euro, privacy, pseudonymity, anonymity, digital payments

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Tomy Lee, for his guidance, critical feedback, and support throughout the research and writing of this thesis. His insights helped me approach the topic with clarity and critical perspective.

I also thank Marc Kaufmann for his constructive comments during my thesis presentation and for challenging me to strengthen key arguments.

Lastly, I'm thankful to my professors and friends at Central European University for creating such an inspiring environment, and to my family and friends for their patience and encouragement along the way.

List of Abbreviations

AML – Anti-Money Laundering

BIS – Bank for International Settlements

CBDC – Central Bank Digital Currency

CFT – Counter-Terrorism Financing

CNIL – Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)

EBA – European Banking Authority

ECB – European Central Bank

EDPB – European Data Protection Board

EDPS – European Data Protection Supervisor

E-Krona – Sweden's Central Bank Digital Currency

EPI – European Payments Initiative

EU – European Union

GDPR – General Data Protection Regulation

IMF – International Monetary Fund

KYC – Know Your Customer

MiCA – Markets in Crypto-Assets Regulation

PBoC – People's Bank of China

SPACE – Study on the Payment Attitudes of Consumers in the Euro Area

Table of Contents

List of Figures

Introduction

The idea of digital money is not new, but it has gained momentum in recent years, especially as central banks respond to the decline of cash and the rise of private digital alternatives like stablecoins. The European Central Bank (ECB) is now developing a digital euro, public money for everyday use, intended to offer the benefits of digital payments while preserving the trust and legal status of central bank currency. According to the ECB, the digital euro will provide "cash-like" privacy. Yet, delivering on this promise is not that simple. Privacy in digital payments must balance data protection, financial oversight, and technical feasibility, all within a complex legal framework.

This thesis asks: *Can and should the digital euro offer comparable privacy to cash within existing EU legal and technical constraints?* This question matters not only because privacy is a legal right in the EU, but because it also shapes public trust in digital institutions.

The thesis proceeds as follows. *Chapter 1* reviews the literature on CBDCs, focusing on legal, technical, and political perspectives on privacy. *Chapter 2* explains why privacy matters in payments, especially in the EU, and outlines the case for a public digital currency. *Chapter 3* assesses whether the digital euro complies with key regulations, GDPR, ePrivacy, AML/CFT, and MiCA, and where legal limits constrain privacy. *Chapter 4* examines case studies from Sweden, China, and the BIS to compare privacy trade-offs across jurisdictions. The conclusion considers whether the ECB's current design can meet both legal requirements and public expectations.

The approach is qualitative and policy-oriented. The method used is primarily qualitative and comparative, drawing on policy papers, technical reports, legal opinions, and prior CBDC implementations. The analysis is structured around thematic chapters addressing legal trade-offs,

technical limitations, and comparative design decisions. By comparing regulatory goals with the ECB's design features, the thesis assesses if cash-like privacy is a realistic and appropriate target.

Empirical data such as adoption preferences or behavioral trust studies are not included as this falls outside the scope of this thesis. The approach instead focuses on evaluating the credibility of design promises using available legal texts, policy documents, and published technical materials.

The findings suggest that the ECB's digital euro design does not offer cash-like privacy and is unlikely to do so under current technical, legal and institutional constraints. While the ECB plans to implement data minimization and pseudonymization, these do not offer full anonymity. Offline functionality is proposed to replicate cash-like privacy but is limited to transactions (€150) to comply with AML, a feature additionally depending on technology currently not available to all users. Legal ambiguity remains as many privacy-related features are not codified but left open to future legislation. This places long-term privacy protections at the risk of political fluctuations. The ECB's absence of privacy guarantees, and so far, not clearly allocated responsibilities, suggests that users may be asked to trust institutions rather than rely on legal protections.

Case studies reinforce these concerns. Sweden's e-krona design avoids anonymity and emphasizes transparency. China's e-CNY uses pseudonymity with state-accessible backdoors, implying surveillance concerns. Tourbillon, while technically advanced, remains a prototype with limited practical application. These cases suggest that strong privacy is possible but politically and technically difficult, and that trade-offs must be carefully evaluated.

This thesis contributes to current debates on CBDC design by focusing on privacy not only as a legal requirement but as a core feature shaping public legitimacy and institutional trust. It builds on policy literature but extends the discussion by critically examining the ECB's privacy claims against design realities. By comparing EU regulatory frameworks with the ECB's proposed model and global CBDC alternatives, this thesis adds an interdisciplinary, policy-oriented perspective to the growing field of CBDC research.

Chapter 1: Literature Review: The Evolving Debate on CBDCs and Privacy

Central bank digital currencies (CBDCs) are at the center of ongoing discussions on the future of money, privacy, and institutional design. The European Central Bank (ECB) presents the digital euro as a complement to cash, claiming it will offer similar privacy and accessibility. However, the literature reveals significant gaps between this promise and the proposed design, suggesting that there is no clear legal basis guaranteeing cash-like privacy.

This review is a synthesis of findings across academic, regulatory, and policy sources into four key themes: (1) the legal framework and its interactions with data protection laws; (2) the technical design and implications on privacy; (3) the ECB's institutional incentives; to tie everything together, there is (4) public trust and normative considerations on digital monetary governance.

1.1. Legal Architecture and EU Law

A key issue raised in the literature is the digital euros compliance with existing European privacy regulations, with the General Data Protection Regulation (GDPR), the ePrivacy Directive and Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) requirements.

To comply with the above mentioned, the ECB has proposed a two-tier model, with intermediaries managing user data, which does not meet the legal standards for anonymity according to research, as the digital euro's data policy allows for re-identification of users (Pendo et al., 2024; Minto, 2025). The joint opinion of the European Data Protection Board and Supervisor (EDPB-EDPS 2023) recommends incorporating privacy-by-design features for at least low-value offline payments, but the ECB has instead settled on implementing pseudonymization for all payments. Yet, offering full anonymity for low-value transactions up to €150 is legally possible, as it complies with existing EU rules, including the GDPR, ePrivacy Directive, and AML regulations.

The ECB has claimed that there is no intention of surveillance from their side, but according to scholars, for privacy privacy protection to be irreversible it must be ensured by technical architecture, not intentions and policy restraints, as those may be altered by future regimes (Kuner, 2017). This concern is important as institutional roles change over time across EU member states.

1.2. Technical Design and Privacy Features

The ECB's technical design is based on a two-tier model, with the ECB managing issuance and settlement, while intermediaries such as banks would interact with users. Despite being described as neutral from a technology perspective, the system is designed as a permissioned and centrally governed network, where only authorized entities are granted access and control, and is typically managed by a central authority (ECB, 2023). The model incorporates privacy-enhancing features by using pseudonymized identifiers to mask user identities, with plans to support limited peer-to-peer anonymous offline payments via smartphones or smart cards (ECB, 2024; BIS, 2023). Researchers argue that this solution replicates existing technologies, adding that special offline features may exclude users without smartphones (BIS, 2023).

Alternative CBDC designs offering enhanced privacy features have already been explored by previous pilots. Sweden's e-krona, which operates within the EU's regulatory environment, incorporates partial privacy protections that align with regional data and financial regulations. Meanwhile, the Bank for International Settlements' Project Tourbillon has explored advanced privacy techniques that allow users to make transactions without revealing their identities, using quantum-resistant cryptography to keep data secure against threats. The ECB has yet to test their solutions, despite the EDPB recommending their start doing bigger-scale pilots (EDPB, 2023).

1.3. The Political Economy of the Digital Euro

The political rationale for the digital euro started from concerns about private currencies like Facebook's Libra in 2019. Over time though, the idea evolved to gaining strategic autonomy and reducing Europe's dependence on foreign payment networks such as Visa, Mastercard, and Pay Pal (ECB 2020; Keating 2025). Scholars argue that this concern alone does not justify the ECB's decision to create a new public digital currency, as the digital euro could add another layer of complexity to Europe's already fragmented payment infrastructure, which mainly relies on external providers. Furthermore, a CBDC with a limited wallet value of €4,000 would not sufficiently address the issue of overreliance on foreign systems (Grünewald 2023). Instead, the suggested solutions include strengthening SEPA Instant or supporting the European Payments Initiative (EPI) which target overreliance directly with less complexity (Brosens 2022; Bruegel 2023).

1.4. Normative Perspectives, Public Trust, and Surveillance Risk

Literature consistently identifies public trust as a critical factor in determining the viability of CBDC adoption (Acquisti et al., 2016). There are concerns that surveillance could become normalized through technical infrastructure since the system design allows it, and institutional limitations can be lifted, a gap that can affect user confidence (Westermeier, 2024; Ratti, 2023).

The ECB's SPACE study (2024) confirms privacy remains a major concern for European citizens, as 43% rank it as a primary feature of the digital euro. This concern is particularly prominent in cash-intensive member states, suggesting a strong cultural attachment to financial privacy. Privacy is a valid concern in this context because digital payments can expose sensitive transaction data, increasing the risk of surveillance, data misuse, or discrimination (Bundesbank 2023).

Chapter 2: Privacy in Digital Payments

2.1. Why Privacy Matters

Money and privacy are not often discussed together, yet the relationship between them quietly shapes consumer behavior in significant ways. A lack of financial privacy can lead to distortions in both economic choices and legal frameworks. From an economic perspective, it may influence consumer preferences, discouraging certain types of transactions or purchases (Borgogno and Colangelo 2022). Legally, the right to monitor individual spending has been widely debated and subject to regulation (Kuner 2017; Lynskey 2015). As a result, insufficient privacy can introduce inefficiencies into the broader economy and raises concerns about excessive government control over personal freedoms (Zuboff 2019).

When individuals avoid purchases due to privacy concerns, businesses operating in these areas may consequently see reduced demand. Alternatively, people may continue spending on sensitive items but shift to informal payment methods like barter or privacy-preserving currencies, pushing transactions into the economic gray zone (Narula 2020; ECB 2021). In both cases, the state loses tax revenue as economic activity moves off the books despite still taking place (Rogoff 2016). Overall, this can affect public finance and market functioning, as the lack of privacy may lower aggregate welfare by changing individual behavior and reducing the effectiveness of fiscal policy.

At the same time, it is important to recognize that individuals often choose to share data with private actors such as commercial banks, FinTech firms, or digital wallet providers in exchange for immediate benefits such as personalized financial services, credit scoring, or targeted offers, all of which depend on access to user data. This exchange is voluntary and based on perceived value. Users retain some control over how their data is used and typically have the option to

withdraw consent. This element of choice is important, since individuals decide which providers to trust, how much information to share, and under what terms. If trust is compromised, they may switch to alternative providers with stronger reputations. On the other hand, private actors have a strong incentive to maintain user trust, as losing it directly affects their competitiveness and market position. This dynamic raises questions in the context of CBDCs, where the user could not simply "opt out" or switch providers. Public trust in the central bank as the issuer, would be essential to be earned through transparency, legal safeguards, and clear limitations on data use (Auer et al. 2020).

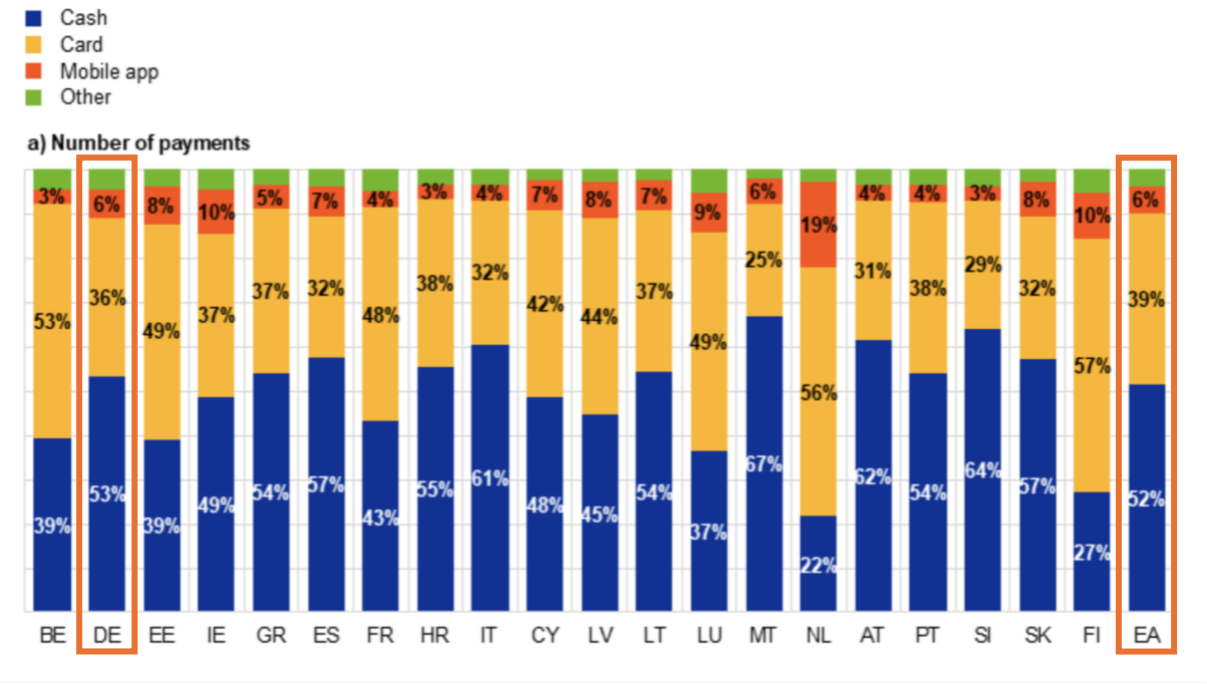
This distinction is important because the ECB has stated its goal to offer privacy protections for the digital euro comparable to those provided by private companies (ECB 2021). However, for public institutions, the question is not if users can control their own privacy, but whether they should have to. If privacy is considered a fundamental right rather than a personal preference, then institutions may have the responsibility to protect it, and not place that responsibility on individuals.

2.2. Privacy in the EU

In several European countries, the experience of financial surveillance under past regimes has left a lasting impact on how people view privacy today. For example, East Germany's Ministry for State Security kept detailed records on individuals, including aspects of their financial and consumer behavior, as part of a broader system of population control (Pohle and Kreutz 2016). Such historical experiences may have contributed to a continued caution toward digital data sharing, especially when it involves financial transactions. Today Europe has robust legal protections that set high standards for personal data security and user privacy, but in the absence of legal constrains, policy makers can change the rules, which is why regulators ask for privacy by design.

Yet privacy is not the only determinant of payment choices. Infrastructure, perceived cost, and habit can also be significant reasons behind it. Recent data from the ECB's 2024 Study on the Payment Attitudes of Consumers in the Euro Area (SPACE) report shows that 52% of point-of-sale (POS) transactions across the euro area are still conducted in cash, as higlighted in *figure 1*. POS transactions consider transactions at a physical location for example in shops, restaurants, service providers, public transport etc.

Figure 1: Payment means used at the POS in 2024



Source: *ECB 2024*

To assess whether this is a necessity or constraint, Germany is used as a reference case due to its economic weight in the euro area and the availability of detailed payment data from the Deutsche Bundesbank, which regularly informs ECB-level research. Cash remains the dominant method for POS payments in Germany, despite card acceptance being available at around 80% of retail outlets (Deutsche Bundesbank 2023). This statistic challenges the assumption that cash is used primarily

due to infrastructure constraints. Instead, it appears that for most transactions, especially those involving low-value or routine purchases under €100, the choice to use cash is voluntary (ECB 2024).

Research identifies three main reasons why people prefer to hold and use cash: ease of transaction, budgeting control, and independence from oversight (Deutsche Bundesbank 2023). Unlike digital transactions, cash allows individuals to retain a degree of anonymity and control. Since amounts used for cash payments according to this research are under €150, they reflect consumers desire to preserve their personal freedom in everyday life, rather than intent to engage in illicit activity.

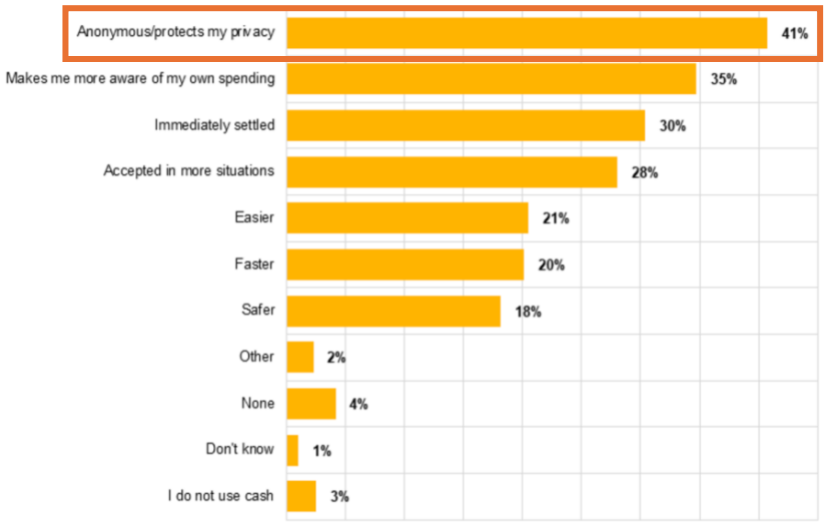
2.3. Making the Case for a CBDC

The persistence of cash suggests that many individuals continue to value payment methods that offer a degree of control, discretion, and autonomy. Any digital alternative, particularly one issued by a public institution, may need to reflect these preferences in order to achieve broad acceptance. While digital systems can offer improvements in efficiency and accessibility, concerns around privacy and personal control remain central. As higlighted in *figure 2*, privacy is now reported as the most significant advantage of cash in the euro area, ahead of speed or convenience.

In this context, the rationale for introducing a digital euro arguably may have to extend beyond questions of technological feasibility. If the ECB seeks to promote widespread adoption, it is be important to consider the broader functions cash currently fulfils, not only as a medium of exchange, but also as a means of maintaining financial independence and limiting exposure to data collection. Otherwise, adoption may be limited if similar attributes are not incorporated into the design of a CBDC. Ensuring trust in the issuer could depend not only on institutional reputation but also on the presence of clear rights and verifiable constraints on data use, as even in well-

regulated democracies, payment data can, be repurposed for uses that go beyond the original intent if not properly regulated (Acquisti et al. 2016; BIS 2023).

Figure 2: Perceived advantages of cash in the euro area in 2024



Source: *ECB 2024*

As this chapter has shown, privacy plays an important role in shaping consumer preferences and trust in digital payments. With the digital euro still in development, there is an opportunity to examine how the ECB's design choices respond to these concerns within the limits of its mandate. The next sections explore whether current proposals find a balance between privacy, regulatory compliance, and the broader expectations attached to public money in a digital context.

Chapter 3: Assessing Constraints on Privacy in the Digital Euro Legal Framework

The ECB reported that the digital euro will offer "cash-like" privacy and align with EU data protection rules. This chapter examines if the proposed design meets this claims, and if yes to what extent, by analyzing its compatibility with the General Data Protection Regulation (GDPR), the ePrivacy Directive, and anti-money laundering (AML) regulations. Furthermore, the EU's Markets in Crypto-Assets (MiCA) will also be assessed to check if the ECB's broader justification for launching a CBDC remains consistent since the regulation of stablecoins and crypto assets.

By deep diving into legal frameworks, this chapter tests how the ECB's promises can be met in practice, as it provides the tools to evaluate trade-offs needed to achieve meaningful privacy within the proposed framework.

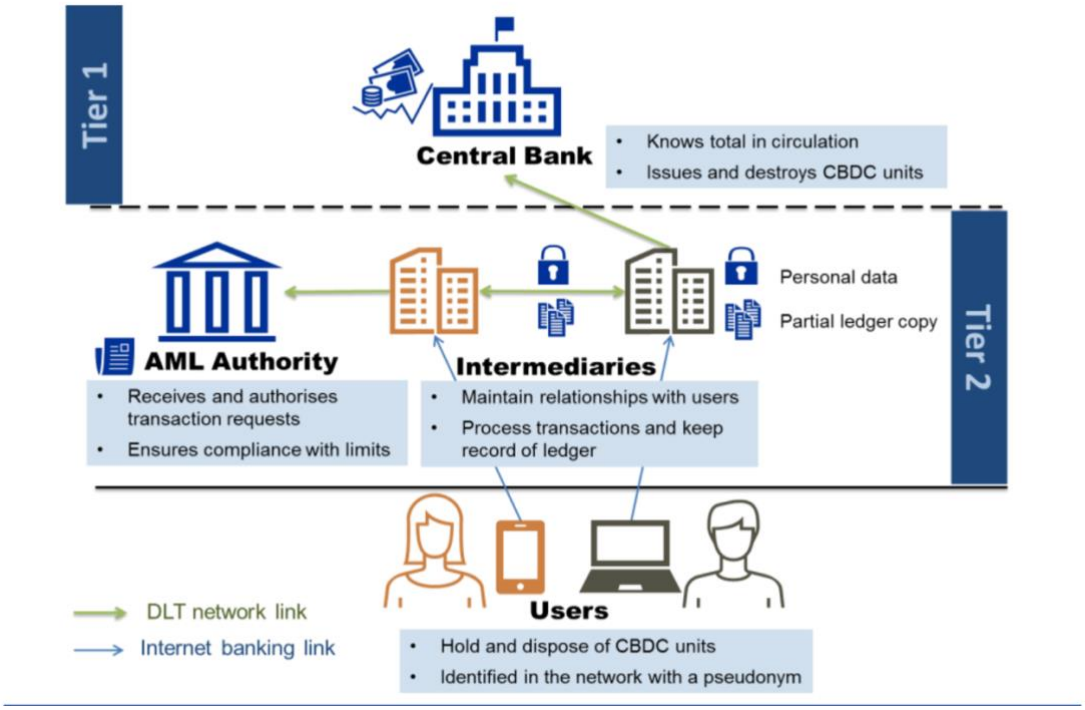
3.1. GDPR and the Limits to Privacy

The strongest form of privacy in payments today is offered by cash. It operates outside digital infrastructure, leaves no transaction trace, and requires no third-party verification. Regulators like the European Data Protection Board and Security (EDPB-EDPS) and France's National Commission on Informatics and Liberty (CNIL) have emphasized that any digital alternative, such as the ECB's proposed digital euro, should aim to preserve a similar degree of anonymity, at least for low-value transactions (EDPB-EDPS 2023; CNIL 2022). While this standard has been acknowledged in EU discussions, the actual design of the digital euro reveals a clear gap between the rhetoric of "cash-like privacy" and what is technologically and legally being proposed.

The GDPR is the main law protecting personal data in the EU. It gives people rights over their data and sets limits on how institutions can collect, store, and use it. The ECB intends to meet GDPR requirements through pseudonymization and role separation. That means intermediaries,

like commercial banks or payment providers, handle user identity, while the ECB only sees pseudonymized data (ECB 2023). This sounds compliant but doesn't guarantee anonymity in practice. Pseudonymized is still personal data and can be re-identified, especially when cross-referenced with other data sets (GDPR Art. 26). In that sense, the ECB's model offers what might be better described as conditional identifiability rather than privacy. The term "cash-like" becomes misleading as it may create the perception of full confidentiality.

Figure 3: Two-tier model and relationship between entities



Source: *ECB 2017*

The technical structure of the digital euro reinforces this dynamic. It's built as a two-tier system as seen in *figure 3.*, with private intermediaries handling users and identity verifications, while the ECB processes payments without directly holding identifying information (ECB 2023; European Commission 2023). On paper, this supports the principle of data minimization. But legally, under the GDPR, even pseudonymized data is still personal data if there's a possibility of re-identification

(GDPR Art. 4(5)). Moreover, the ECB will have access to transaction metadata, such as time, location, or frequency, which can be revealing when combined with external information (Pendo et al. 2024). Although the ECB may not intend to monitor individuals, the system architecture allows it in principle. This suggests that the right to privacy does not depend on intentions alone, but also on what is technically feasible.

The two-tier infrastructure also ties into the unresolved issue of legal controllership. Under EU law, data controllership defines who decides the means and purposes of processing (GDPR Art. 4(7)). But in the digital euro model, control is split into two. Intermediaries hold personal data, while the ECB issues the CBDC and processes payments. The division blurs accountability as users have no guidance who to approach in case of arising issues. Clarifications are needed as vague roles might weaken transparency and legal mechanisms (EDPB-EDPS 2023).

A further concern is data retention. Under GDPR, data should not be stored longer than necessary (Art. 5(1)(e)). But anti-money laundering laws require financial institutions to retain payment data for five to ten years. The ECB's current proposal may go beyond this requirement, as it may allow intermediaries to hold on to user data for extended periods (European Commission 2023). This is legally justifiable, but might become problematic in practice, as over time, stored data becomes a liability vulnerable to breaches, misuse, or repurposing.

3.2. Offline Payments and the ePrivacy Directive

To address rising privacy concerns, the ECB has proposed an offline functionality for the digital euro aimed to replicating cash's anonymity, especially for low-value transactions (ECB 2024; ECB 2022). Offline functionality would process transactions locally on a user device without contacting the ECB or intermediaries, avoiding metadata collection and aligning with the ePrivacy Directive's confidentiality standards (Directive 2002/58/EC, Art. 5). Since ePrivacy prohibits tracking

metadata like time, device, or location without explicit consent, offline payments seem like a legal workaround that could solve privacy concerns. The ePrivacy Directive works alongside GDPR but focuses more narrowly on privacy in digital communications. It's offers additional protection especially around metadata and consent, but it hasn't been fully updated in years.

But this solution seems narrow as the offline function is only available for low-value payments, with a €150 cap set to satisfy AML rules (European Commission 2023). This makes anonymity a conditional right available only in certain situations and for certain amounts, not quite like cash.

Additionally, even when offline payments comply with regulations, they currently depend on specific hardware and secure elements embedded in some user devices only. Data shows that, in 2020, only around 35% of smartphones sold had this technology, with projections suggesting this may rise to 50% by 2025 (Counterpoint 2021). This means those without compatible devices, often older adults, low-income groups, or people in rural areas, could be excluded by default from this feature. With offline functionality, the ECB avoids violating privacy law, while indirectly deepening digital inequality by tying privacy access to specific.

Further complicating the matter are fallback identification mechanisms designed for fraud prevention (ECB 2023). If a user loses their device or behaves suspiciously, it seems authorities may be able to re-link a transaction to an identity. These mechanisms are presented as security features, but they also show that even offline anonymity is not in fact anonymous. The exact conditions under which privacy is lifted are not clearly defined, leaving space for interpretation.

This design has been criticized by research, as there are warnings that political compromise on anonymity cannot replace clear and enforceable legal data protections, as evident from fallback mechanisms (EDPB-EDPS 2023; CNIL 2022). Similarly, the Berlin Group argues that if fallback

systems are built in by default, privacy is no longer protected by design even if no direct tracking occurs (Berlin Group 2024). Their concern is not about intentions alone but architecture because if a system is built to allow traceability, the limit of privacy in the digital euro is set by the gap left between compliance and protection.

3.3. Anti-Money Laundering Obligations

The legal foundation of AML/CFT in the EU makes full anonymity functionally unfeasible for any digital currency issued or managed by a regulated institution. Under Directives 2015/849 and 2018/843, payment service providers are obligated to implement know your customer (KYC) protocols, monitor transactions, and report any suspicious activity. These requirements apply regardless of the technology used weather it is digital, offline, or otherwise. In principle, even offline transactions, if later suspected to be suspicious, must be traceable to comply with these obligations. Although this is not possible with cash either.

While privacy-enhancing features may exist at the user interface level (e.g., pseudonymity and offline anonymity), they can be overridden at the system level if legal mandates require that. Any claim to anonymity is therefore limited by default if it wants to comply with AML.

This constraint reflects the ECB's strict policy stance. In some public statements, the ECB has stated that full anonymity is not a desirable feature for the digital euro due to its incompatibility with AML/CFT goals (ECB 2022). This implies privacy is not treated as a foundational right within the digital euro architecture, but as a conditional feature that may be revoked when compliance pressures arise. Even in "offline" mode, the ECB keeps mechanisms to re-identify users under certain conditions (ECB 2023). Therefore concerns raised in the ePrivacy are reinforced.

The ECB's messaging complicates this picture further as references to "cash-like privacy" seem to only appear to manage public concerns, yet the digital euro's technical design contradicts this

claim. True cash-like anonymity means no trace, no re-identification, and no fallback linkage. The digital euro cannot offer this due to legal compliance constraints, so what is marketed as anonymity is only controlled pseudonymity, private only unless and until authorities choose otherwise.

This tension in data related topics is known by what scholars have defined "compliance creep." Under GDPR, data processing must be lawful, necessary, and proportionate (GDPR Art. 5; Recital 39), but AML rules are overly interpreted, especially in contexts involving national security or financial integrity, as more data collection is justified by intentions to identify all risks. The ECB may have in mind that if there are exceptions to surveillance into the technical infrastructure, this may be repeated. Leaving this open gives flexibility to institutions but offers no clear guarantees for users.

Scholars warn that in such cases privacy can become dependent on future political decisions which can shift due to economic crises or other disruptions (Minto, 2025; Westermeier, 2024). As PayTechLaw (2023) points out, the ECB may be leveraging AML obligations not only for legal compliance but also to maintain operational and informational control. In this context, compliance goes beyond legal minimums and may start turning into a governance strategy.

3.4. The Role of MiCA in Reframing the ECB's Justification for a CBDC

The introduction of MiCA has changed the policy landscape in which the digital euro was proposed. When the ECB first advocated for a CBDC, it framed the move as a defensive response to the increase of private stablecoins, particularly Facebook's Libra. The perceived risk was that these unregulated alternatives could erode the euro's dominance in the EU payments ecosystem, weaken the transmission of monetary policy, and fragment authority (ECB 2020). To address this risk, a CBDC was proposed so that it would ensure trust, stability, and regulatory oversight.

However, MiCA now directly addresses the regulatory gaps that previously justified this position. Under Regulation (EU) 2023/1114, stablecoin issuers face strict obligations as they must be authorized entities, hold sufficient reserves in euros, maintain robust governance, and have ongoing supervision. Articles 43 to 47 outline these requirements in detail, establishing a legal infrastructure that obligates private issuers to many of the same expectations as traditional financial institutions. In this context, the threat once posed by unregulated stablecoins seems neutralized.

In response, the ECB has switched their narrative as they now emphasize Europe's overdependence on foreign payment infrastructures such as Visa, Mastercard, and Big Tech firms as a reason for pursuing the digital euro. ECB officials have framed the project as essential to achieving "strategic autonomy" in the financial sector (Panetta 2025). Yet, while this reason may be politically reasonable, it lacks the urgency of the initial stablecoin threat. Researchers suggest that policy goals can be addressed through regulation alone, challenging the assumption that a new currency is needed to address this issue (Bruegel 2023).

Other ideas include the ECB and the Commission concentrating on enhancing the current regulatory tools and infrastructure, rather than introducing a digital currency with unclear benefits and high surveillance risks (Positive Money Europe, 2021). In this context, the European Payments Initiative (EPI) was launched to create a pan-European payment system and reduce reliance on non-EU providers. Its digital wallet, Wero, already went live in 2024 and offers instant payments across Europe, seemingly addressing some of the same goals the digital euro hopes to meet in the coming years. A report by Deutsche Bank additionally warned that the digital euro may duplicate what EPI already does if both projects move forward without coordination (Deutsche Bank Research 2023). This report raises the question are two solutions necessary if one is already in use, and the second offers a wallet of €4,000, making it less functional (Grünewald 2023).

3.5. Is Meaningful Privacy Possible Under EU Rules?

A three-part framework is used for this analysis. Legal trade-offs show what is permitted or restricted by law. Technical trade-offs show how feasible privacy is in practice. Economic trade-offs show how users and institutions will react to privacy limits, affecting adoption and trust. An overview of the analysis and policy implications can be seen in *figure 4*.

Legal Trade-Offs

Three regulatory frameworks intersect in complex ways: the GDPR, the ePrivacy Directive, and the AML/CFT directives. The GDPR (Arts. 5, 6) allows the collection of personal data under clear conditions, purpose limitation, minimization, and accountability. The ePrivacy Directive (Directive 2002/58/EC, Art. 5) is stricter, as it requires consent to collect metadata such as location, time, or device identifiers. In contrast, AML/CFT laws (Directive 2015/849; 2018/843, Arts. 11–13) requires full traceability of digital transactions above €150, with identification and monitoring obligations, just in case.

Coordinating these frameworks is legally possible only through layered designs, as seen in the two-tier infrastructure (see figure 3.). However, this structure does not offer cash-like anonymity. One approach to achieve a balance is limiting anonymity to low-value offline payments, making it acceptable under AML thresholds, while using pseudonymization for higher-value transactions. However, under GDPR Art. 4, pseudonymized data is still personal and must have a responsible controller. This would obligate the ECB to assign clear roles and accountability across its two-tier model. Lastly, there is device-level data collection for offline payments which is necessary for fraud prevention. This would violate ePrivacy unless it is clearly defined as strictly necessary under AML with clear justifications, or consent must be requested by users to collect this data. Clearly defining for how long data can be stored would also fall into this design choice.

Technical Trade-Offs

Technology limitations revealed that privacy may also introduce inclusion issues. Offline functionality is the only feature offering cash-like anonymity, but so far it appears to depend on specific smartphones with secure hardware or dedicated smart cards. If full privacy depends on access to compatible technology and it risks excluding those without such devices undermining the digital euro's claim to universality. The ECB is faced with finding a technical solution allowing this function to work across different devices, subsidize devices to users to eliminate discrimination, or sacrifice anonymity as a consequence to high costs of these solutions.

System visibility is another issue, as full privacy limits the ECB's ability to monitor payment flows, which may be important in times of crisis. However, the opposite extreme offering too much oversight risks triggering public concern over surveillance and restrictions. This may lead users to exit the system entirely in favor of cash, crypto, or foreign currencies. Excessive control could even raise inflation fears if users believe the ECB can influence or manipulate spending, considering how consumer expectations shape inflation (ECB 2022; Mankiw et al. 2020).

Economic Trade-Offs

The ECB's messaging has implied privacy in the digital euro to be "like cash," even though full anonymity is legally off the table as seen from analysis so far. This gap between expectation and delivery could harm public trust when the digital euro is presented at a national scale if not managed carefully.

Moreover, the digital euro may be a redundant and complicated solution. Since 2023, MiCA (Regulation 2023/1114) has imposed strict oversight on stablecoins, it closed many of the gaps that originally justified a public alternative. And with the European Payments Initiative (EPI)

launching "Wero," a pan-European digital wallet designed to reduce dependence on foreign payment networks directly, it seems that a simpler solution is already available to resolve remaining concerns for overreliance. Since privacy in the digital euro is limited, and alternatives already meet the goals of sovereignty and innovation, its added value has become harder to justify.

Figure 4: Trade-Off Matrix

Legal Trade-Off	Tension Area	Policy Insight
Privacy vs. AML Compliance	Anonymity vs. traceability	Only low-value privacy is feasible under EU law
Privacy vs. Data Accountability	User protection vs. fragmented roles	Assign clear data controllers
Privacy vs. ePrivacy Compliance	Metadata collection vs. consent	Clarify metadata use and consent mechanisms

Technical Trade-Off	Tension Area	Policy Insight
Offline Privacy vs. Exclusion	Accessibility vs. secure infrastructure	Ensure inclusive access to privacy features
Privacy vs. System Visibility	User protection vs. monitoring power	Balance surveillance with public trust

Economic Trade-Off	Tension Area	Policy Insight
Privacy Promise vs. Delivery	Public expectations vs. real design	Avoid overpromising to preserve trust and adoption
CBDC vs. Regulated Alternatives	New public tool vs. existing options	Reassess added value beyond MiCA and EPI

Source: *Author*

Chapter 4: Case Studies: Privacy, Design, and the Digital Euro in Comparative Perspective

In order to evaluate the ECB's digital euro, this chapter looks at three central bank digital currency (CBDC) pilots: China's e-CNY, Sweden's e-krona, and the BIS-led Project Turbillon. Every example presents a unique implementation model of a CBDC influenced by institutional capabilities, regulatory frameworks, and national interests. The emphasis is on design decisions, legal restrictions, and privacy trade-offs.

This chapter explores if the ECB's cautious approach to privacy represents a conservative view of its policy environment or a necessary limitation, as tested in parallel to existing pilots.

4.1. Sweden – e-krona

Sweden's e-krona pilot began in 2017 as a response to the country's rapid decline in cash usage. The Riksbank initiated the pilot to ensure that state-issued money remains relevant in a digital economy and to reduce reliance on private and Big Tech-controlled payment systems (Riksbank 2020). The project was structured in four phases, using a permissioned distributed ledger technology (DLT), a blockchain like system that only approved actors can access. Both online and offline functionality was included in their design.

Two of the phases have already tested offline anonymous payments using shadow wallets, which turned out to be technically feasible, but complex because of settlement protocols (Riksbank 2023; Riksbank 2024). They found out that reconciling payments when offline is not possible, meaning the transaction could happen when offline, but then the balance would get updated only once the device is online again, which raised concerns of double-spending.

In case the project gets implemented, the Riksbank would be responsible for issuance and settlement of e-krona. The Riksbank has made it clear that anonymity will not be allowed even if

technically possible (Riksbank 2021). Instead, it would be fully compliant with the GDPR and Swedish financial secrecy laws. This means intermediaries must perform full KYC under AML/CFT rules, while personal data is processed as required by the GDPR and protected under the Swedish Payment Services Act (Lind 2023). In simple terms, intermediaries verify user identity, while personal data is stored and can only processed for specific legal purposes. However, DLT technology may lead to storing more personal data than current private platforms, which raises concerns about data minimization under the GDPR (CoinDesk 2020).

Despite transparency through official reports and updates, public adoption of the e-kronor has been limited. The Riksbank presented the e-krona as a complement and not a replacement for cash. This may be because digital payment tools such as Swish are already widely used, rather than privacy concerns and fear of surveillance. In fact, Swedish users seemed to associate anonymity with illicit transactions and money laundering, and instead prefer that authorities have control to intervene in such cases (IMF 2022; Riksbank 2023).

Sweden shows that a technically feasible and privacy aware CBDC can be developed within a strict regulatory framework, although with challenges, but legal and technical compliance alone are not sufficient if the CBDC does not offer clear value to users, in which case adoption is unlikely.

4.2. China – e-CNY

China's e-CNY is among the most advanced CBDC projects globally. Pilots began in 2020 across cities such as Shenzhen, Suzhou, and Beijing, and by mid 2024, transaction volume had reached trillions of yuan (Atlantic Council n.d.). The main goals of this project are to modernize the monetary system, improve financial inclusion, and reduce reliance on dominant private platforms like Alipay and WeChat Pay. Some analysts also view it as part of China's long-term strategy to reduce reliance on SWIFT and strengthen monetary control (Kosse and Mattei 2022; BIS 2021).

The e-CNY uses a two-tier model. The People's Bank of China (PBoC) issues the currency, while banks and FinTech firms distribute it (PBoC 2021). The system supports offline payments using hardware wallets such as SIM cards, wearable devices, and dedicated cards (Ledger Insights 2023). Although the exact ledger structure is not public, it is assumed to be centralized and highly programmable, which makes high scalability possible as evidenced from a high number of transactions, but also gives full control to the state over data (Auer et al. 2023).

Privacy is based on what Chinese authorities call "controllable anonymity." This means user identities are hidden from merchants but remain visible to the state, especially for AML compliance and national security reasons (PBoC 2021). However, there is no legal equivalent to the GDPR in China, and no clear mechanisms exist for users to challenge how their data is used. In practice, the centralized system allows for financial data to be stored into broader state surveillance infrastructure, with minimal institutional safeguards (Xu 2022).

China managed to get higher adoption using subsidies and lotteries to distribute wallets and roll out pilots, but public adoption still remained relatively low when compared to Alipay and WeChat Pay, which accounts for over 90% of mobile payments (SCMP 2023). The e-CNY is being promoted by the state media as a symbol of modernization and national strength, but there seems to be no public debate challenging the suggested design. This can only mean two things, either the public is satisfied with what they received, or there is no room for complaints. The adoption rate compared to competition, may be enough to identify which case is more likely true.

4.3. BIS and Project Tourbillon

The Bank for International Settlements (BIS) plays a normative role in shaping global approaches to CBDC design. While it does not issue a CBDC itself, BIS acts as a technical advisor and a policy coordinator. It promotes core design principles focused on monetary stability, financial inclusion,

as well as technological neutrality (BIS 2021). BIS uses Tourbillon as a thought experiment not a definitive model, to deliver a recommendation to central banks that CBDCs should complement existing financial infrastructure, not replace it. This ensures the transition to digitalization is gradual, as it minimizes disruption and maintains stability (BIS 2022).

Privacy is an important feature in BIS publications, it is not framed as a binary variable between anonymity and surveillance, bur as a balance between individual rights and legal obligations. This means full anonymity is rejected because it would violate global rules that are meant to stop money laundering and terrorism financing. To manage this, BIS uses a tiered identity system requiring minimal KYC for low-value transactions while high-value transfers require full identity checks (BIS 2021). This model minimizes data collection, but still allows authorities to investigate serious financial crimes. Data is collected, but this does not mean that authorities have automatic access.

BIS demonstrates how cryptography can ensure privacy, as it uses zero-knowledge proofs (ZKPs) and Merkle tree structures to process payments without exposing user identity or transaction metadata to intermediaries (BIS 2024). In practice, this allows users to retain control over their payment data while allowing regulators to identify suspicious patterns through audited access mechanisms. However, authorities are not allowed to see user data automatically. In order to access sensitive data, they need legal approval to gain access to special keys. The keys are used to record logins each time the data is accessed so authorities are held accountable for accessing the data.

One important factor is raised by BIS, as they highlight this project is only a demo that shows privacy in CBDCs can work in theory if advanced cryptography is used. But having the technology is not sufficient as countries still need to have the right laws, institutions, and governance to make sure protocols are respected (BIS 2022). This means that even if the system protects the data,

governments must follow legal procedures to access it, otherwise even the most advanced cryptography is meaningless.

The BIS raises caution for central banks developing CBDCs, as they advise them to move slowly, communicate clearly with the public, and align design choices with existing legal frameworks. They also reveal the cryptography used for this project is computationally expensive, as more processing power is required for basic payments, which challenges scalability (BIS 2022; BIS 2024). However, the message from this experiment is clear. The challenge faced is political rather than technological. Without institutional trust, even the best cryptography cannot guarantee privacy.

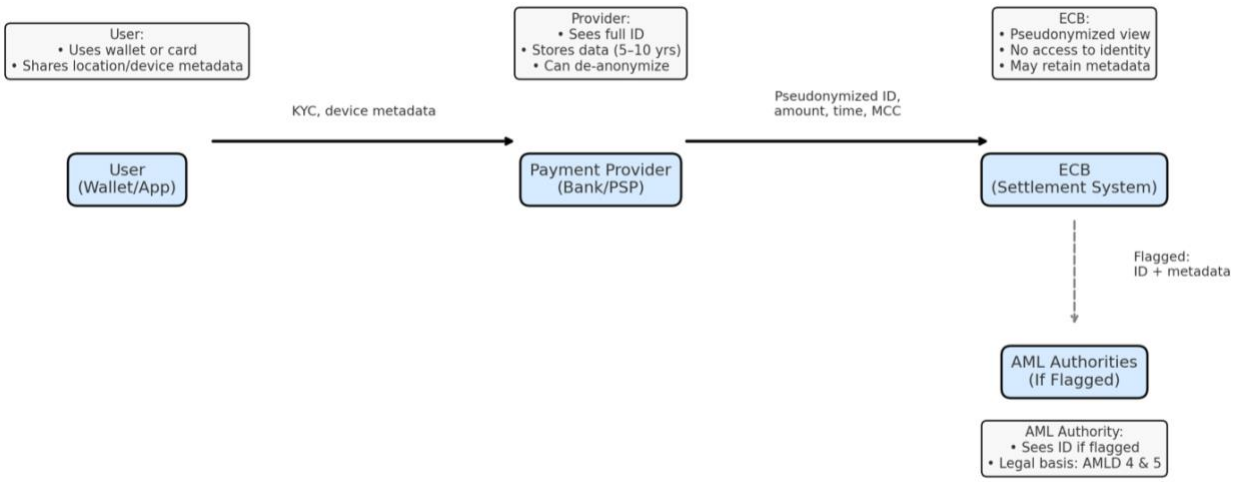
4.4. How Data Flows in a Digital Euro Transaction

Understanding how a digital euro transaction flows from initiation to settlement, makes it easier to identify in which steps privacy risks may arise. *Figure 5* is a simplified roadmap of a digital euro transaction from initiation to end. The user initiates a payment through a wallet, app, or smart card. The transaction is then processed through a two-tier structure. The payment provider or the first tier, usually a commercial bank, verifies the identity (KYC) and links the transaction to a pseudonymized identifier. The transaction is then sent to the ECB's system for settlement. The ECB receives a pseudonym with the amount spent, time of transaction, and possibly a merchant category code showing the location but not items bought (ECB 2023).

If this transaction exceeds certain thresholds or if it has a suspicious pattern, then it is flagged. This is the point when intermediaries may have a legal obligation to de-pseudonymize the user and share the identity of the payer with relevant authorities which are defined under AML obligations. But if there are no triggers for the transaction, personal details stay with intermediaries. Intermediaries are expected to store personal transaction data for 5 to 10 years under AML regulations. The ECB claims it does not store any identifying data, but metadata may still be

retained for system integrity or fraud detection. This makes it important that protections are enforced by design, not just promised (ECB 2023; ECB 2024).

Figure 5: Digital Euro Transaction Flow and Data Access



Source: *Author*

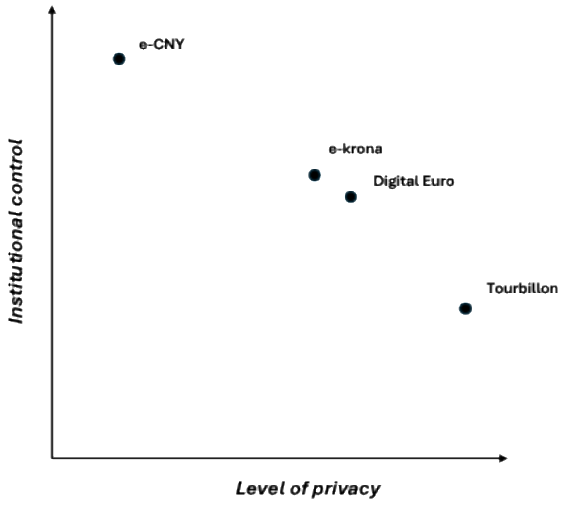
Even if current laws limit access to identity, privacy is protected only for as long as the legal framework stays in place. If rules change, either during a crisis or political shifts, data collected for AML could be repurposed.

In a worst-case scenario, a government could use this system to track political opponents, block transactions based on political activity, or freeze accounts. While this is unlikely in the EU today, the system must be designed to prevent such abuse from being technically possible in the future.

4.5. Scenario Analysis: What Could go Wrong?

The digital euro is designed with mechanisms that protect privacy under current legal constraints, but as seen from the BIS Tourbillon pilot, institutional guarantees cannot shield users from data abuse if political conditions change in the future. This is why privacy risks must be assessed not only against present frameworks, but also based on what the underlying architecture enables under future governments.

Figure 6: CBDC Privacy-Control Trade-Off Landscape



Source: *Author*

Figure 6 synthesizes case studies discussed in this chapter, mapping privacy on the X-axis and institutional control on the Y-axis. For this purpose, privacy refers to the extent to which user identity and transaction data are protected from state or institutional access, ranging from full anonymity (right) to full surveillance (left). Control reflects the technical and institutional capacity to enforce AML/KYC compliance, introduce programmability, and manage system scalability. Positioning is based on design features and institutional context, not quantitative metrics. Similar conceptual mappings are used in ECB and BIS publications (BIS 2023; ECB 2023), aiming to illustrate systemic trade-offs at a glance.

e-CNY is positioned at the extreme, offering minimal privacy, maximum control. The PBoC maintains direct, real-time oversight over transactions, with "controllable anonymity". It is integrated with social credit infrastructure and digital IDs, suggesting that it may have been designed with surveillance in mind (PBoC 2023).

e-krona is placed moderately on privacy but high in control. While it offers no anonymity and full KYC, the Riksbank is accountable and transparent. Political abuse is unlikely under current democratic norms, though technically feasible (Riksbank 2023). The use of blockchain also raises data retention concerns as it stores more data than necessary, conflicting the GDPR.

The digital euro is positioned based on current design plans. Compared to the e-krona, it offers slightly more privacy, data is pseudonymized and stored by intermediaries, not on a blockchain or directly by the ECB. Offline transactions are possible in low values but may be traceable depending on final design. Expanded surveillance is possible under future policy shifts, but unlikely (ECB 2023).

Tourbillon represents the inverse, offering strong privacy and minimal institutional control. Advanced cryptographic techniques limit both traceability and programmability. Surveillance risk is minimized, but it comes at the cost of reduced scalability and speed (Chaum et al. 2021). Additionally, the technology used is quite expensive, challenging the cost/benefit balance with privacy.

Tradeoffs clearly depend on different factors, such as user preferences, government motivation, as well as technical possibilities. But the balance of them also determines if a CBDC can go from offering privacy to no privacy. If privacy is not designed by default, changes can be made. This is not theoretical. Canada's trucker protests saw financial accounts frozen without court orders (Kassam 2022). The Apple–FBI case (2016) highlighted institutional pressure to break privacy protections for broader state access. These examples show that privacy must be hardcoded, as it clearly shows policy-based guarantees can weaken under pressure (Ratti 2023; Zarouali et al. 2021).

Conclusion

This thesis has examined whether the digital euro can and should provide privacy comparable to cash within the existing legal, technical, and institutional frameworks of the European Union. Through a qualitative and comparative analysis, it has become clear that the ECB's current digital euro design, trades off cash-like privacy for regulatory compliance. While data minimization and pseudonymization still offer some level of privacy, they do not achieve full anonymity. The proposed offline transaction limits, constrained by AML regulations and technological availability, further restrict the extent of privacy achievable. Additionally, the lack of explicit legal guarantees and the open-ended nature of privacy-related regulation introduce uncertainty, leaving privacy protections vulnerable to future political and regulatory changes.

Comparative case studies from Sweden, China, and BIS prototypes highlight that strong privacy in CBDCs is both technically feasible and politically challenging. These examples illustrate that design choices reflect broader trade-offs between privacy, transparency, and financial oversight. The digital euro's model leans toward regulatory compliance and institutional trust over absolute user anonymity, reflecting a cautious approach consistent with EU regulatory priorities but at the cost of public privacy expectations.

From a policy perspective, these findings suggest that EU policymakers must clarify the legal framework around privacy and digital currencies and consider how to enhance transparency and institutional trust without compromising regulatory goals. The digital euro's privacy limitations should inform ongoing debates on CBDC design and emphasize the need for robust governance mechanisms that maintain user confidence while addressing financial integrity risks.

This research contributes to the broader discourse on CBDCs by critically assessing privacy not only as a regulatory requirement but as a fundamental component of digital currency legitimacy

and adoption. Future research could explore user perceptions of privacy trade-offs and the economic implications of alternative CBDC architectures, providing further insight into the design choices shaping the digital future of money.

Bibliography

Atlantic Council. n.d. *Central Bank Digital Currency Tracker*. https://www.atlanticcouncil.org/cbdctracker/.

Auer, Raphael, and Rainer Böhme. 2020**.** "The Technology of Retail Central Bank Digital Currency." *BIS Quarterly Review* https://www.bis.org/publ/qtrpdf/r_qt2003j.htm.

Auer, Raphael, Jon Frost, and Leonardo Gambacorta. 2023. "Why So Many Central Bank Digital Currency Projects? A Turbulence View." *BIS Working Papers*, no. 1072. https://www.bis.org/publ/work1072.pdf.

Bank for International Settlements (BIS). 2021. *CBDCs: Financial Stability Implications*. https://www.bis.org/publ/othp38.pdf.

Bank for International Settlements (BIS). 2023. "Project Tourbillon: Privacy in CBDC Transactions." *BIS Innovation Hub*. https://www.bis.org.

Berlin Group. 2024. *Privacy and Central Bank Digital Currency: Position Paper by the International Working Group on Data Protection in Technology*.

Borgogno, Oscar, and Giuseppe Colangelo. 2022. "Data, Innovation and Competition in Finance: The Case of the Access to Financial Data." *Journal of European Consumer and Market Law*.

Brosens, Marc. 2022. "Why a Digital Euro Is Not Europe's Top Priority." *Bruegel Policy Paper*.

Bruegel. 2023. "Do We Still Need a Digital Euro?" *Bruegel Policy Brief*. https://www.bruegel.org.

Chomczyk Penedo, A., et al. 2024. "The Digital Euro and Data Protection: Legal Limits of Pseudonymisation." *European Law Journal*.

CNIL. 2022. "Digital Euro: What Is at Stake for Privacy and Personal Data Protection?" https://www.cnil.fr.

Counterpoint Research. 2021. "Podcast: 50% of Smartphones Will Have Embedded Hardware Security by 2025." https://www.counterpointresearch.com/insights/podcast-50-percent-smartphones-embedded-hardware-security-2025.

Deutsche Bank Research. 2023. *European Autonomy in Payments: Digital Euro Is Not Enough*. Frankfurt am Main: Deutsche Bank AG. https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000528363.pdf.

ECB. 2017. *Exploring Anonymity in Central Bank Digital Currencies*. MIP InFocus, December 19. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.en.pdf.

ECB. 2021. *Eurosystem Report on the Public Consultation on a Digital Euro*. Frankfurt: ECB.

ECB. 2022. *Study on the Payment Attitudes of Consumers in the Euro Area 2022 (SPACE)*. Frankfurt: ECB.

ECB. 2023. *Privacy Explainer: Digital Euro and Privacy*. Frankfurt: ECB.

ECB. 2023. *Stocktake Report on the Investigation Phase of the Digital Euro*. Frankfurt: ECB.

ECB. 2024. "Progress on the Preparation Phase of a Digital Euro – First Progress Report." Frankfurt: ECB. https://doi.org/10.2866/10580.

ECB. 2024. *Progress on the Preparation Phase of a Digital Euro – First Progress Report*. Frankfurt: ECB. https://doi.org/10.2866/10580.

ECB. 2024. *Study on the Payment Attitudes of Consumers in the Euro Area 2024 (SPACE)*. Frankfurt: ECB. https://doi.org/10.2866/9860161.

European Central Bank (ECB). 2020. *Report on a Digital Euro*. Frankfurt: ECB. https://www.ecb.europa.eu.

European Commission. 2023. *Markets in Crypto-Assets Regulation (MiCA) – Regulation (EU) 2023/1114*.

European Commission. 2023. *Proposal for a Regulation on the Establishment of the Digital Euro*. COM(2023) 369 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0369.

European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). 2023. *Joint Opinion 02/2023 on the Digital Euro Proposal*.

European Parliament and Council. 2002. *Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive)*. *Official Journal of the European Communities*, L201.

European Union. 2016. *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*. *Official Journal of the European Union*, L119.

Fan, Yifei. 2020. "Developing and Regulating the E-CNY." *People's Bank of China*. http://www.pbc.gov.cn.

Godschalk, Hugo. 2024. "Digital Euro – No Full Anonymity. Why Not?" *PayTechLaw Blog*. April 10, 2024. https://paytechlaw.com/en/digital-euro-no-full-anonymity/.

Grünewald, Seraina, and Economic Governance and EMU Scrutiny Unit**.** 2023. *A Legal Framework for the Digital Euro*. Edited by Donella Boldi. PE 741.518. Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/741518/IPOL_IDA(2023)741518_EN.pdf.

IMF (International Monetary Fund). 2022. *Sweden: Technical Assistance Report—Central Bank Digital Currency*. https://www.imf.org.

IMF 2024. "CBDCs: Balancing Innovation and Regulation." Washington, DC: IMF.

Kosse, Anneke, and Ilaria Mattei. 2022. *Gaining Momentum — Results of the 2021 BIS Survey on Central Bank Digital Currencies*. BIS Papers No. 125. Basel: Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap125.pdf.

Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey. 2017. *The GDPR: A Commentary*. Oxford: Oxford University Press.

Kuner, Christopher. 2017. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.

Ledger Insights. 2023. "China Trials SIM-Based e-CNY Digital Yuan Wallets." *Ledger Insights*, March 6, 2023. https://www.ledgerinsights.com.

Lind, Elin. 2023. "Data Protection and Confidentiality in the Swedish E-Krona." In *Digital Currency and Financial Secrecy*, edited by M. Andersson, 82–94. Stockholm: Norstedts Juridik.

Lind, Helena. 2023. *E-Krona: Sweden's Central Bank Digital Currency*. Uppsala University. https://www.diva-portal.org/smash/get/diva2:1726955/FULLTEXT02.pdf.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

Mankiw, N. Gregory, David Romer, and David N. Weil. 2020. *Principles of Economics*. 9th ed. Boston: Cengage Learning.

Minto, Andrea. 2025. "Digital Euro and the GDPR: A Critical Assessment of ECB Design Choices." *Journal of European Financial Regulation*.

Narula, Neha. 2020. "Privacy in Payments: A User-Centered Perspective." MIT Digital Currency Initiative. https://dci.mit.edu.

Panetta, Fabio. 2025. "The Governor's Concluding Remarks: Annual Report 2024." Banca d'Italia. https://www.bancaditalia.it/pubblicazioni/interventi-governatore/integov2025/en-cf_2024.pdf.

PayTechLaw. 2023. "Digital Euro – No Full Anonymity. Why Not?" https://paytechlaw.com.

People's Bank of China (PBoC). 2021. *Progress of Research & Development of E-CNY in China*. http://www.pbc.gov.cn.

Pohle, Julia, and Thorsten Thiel. 2016. "Data Protection and Digital Rights in Authoritarian Regimes: The Case of East Germany." *Internet Policy Review*.

Positive Money Europe. 2021. *Will the Digital Euro Respect Citizens' Privacy?* Brussels: Positive Money Europe.

Preibusch, Sören. 2015. "Privacy Behaviors After Snowden." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2558146.

Ratti, Davide. 2023. "Central Bank Digital Currencies and Financial Surveillance." *Digital Rights Law Review*.

Riksbank. 2021. *E-Krona Pilot Report 1*. https://www.riksbank.se.

Riksbank. 2022. *E-Krona Pilot Report 2*. https://www.riksbank.se.

Riksbank. 2023. *E-Krona Pilot Report 3*. https://www.riksbank.se.

Riksbank. 2024. *E-Krona Pilot Report 4*. https://www.riksbank.se.

Rogoff, Kenneth. 2016. *The Curse of Cash*. Princeton: Princeton University Press.

Savage, Charlie. 2016. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone." *The New York Times*, February 17, 2016. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

SCMP. 2023. "China's Digital Yuan Adoption Lags Behind Private Payment Giants." *South China Morning Post*, July 14, 2023. https://www.scmp.com.

Westermeier, Chad. 2024. "Programmability and the Politics of the Digital Euro." *Internet Policy Review*.

Xu, Chenggang. 2022. "Data Governance in China: Financial Data and State Power." *Journal of Chinese Political Economy* 5(2): 111–127.

Zarouali, Brahim, et al. 2021. "Digital Nudging and Surveillance." *Media and Communication* 9(2): 302–311.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York: PublicAffairs.