



March 2026

From Voluntariness to Oversight? The Story of Digital Identity in the EU

Jan Rovenský
Abstract

The European Union presents its digital identity wallet as a voluntary, decentralized, and user-controlled system. By contrast, the United Kingdom's proposed BritCard envisages a mandatory digital identity linked to immigration enforcement and labor market controls. The BritCard case illustrates how digital identity initiatives, initially justified in terms of efficiency and administrative simplification, can evolve into instruments of pervasive monitoring. As the current EU model expands, incorporates new obligations, and becomes increasingly interconnected with public and private services, it could eventually mutate into a similar form of comprehensive control and surveillance. The decisive factor determining its long-term trajectory will be whether it retains the principles of voluntariness, privacy protection, and citizen control over data.

Key Takeaways

- **Fewer Cash Payments:** Cashless transactions continue to rise, and in the Czech Republic most financial operations already take place digitally. Still, only 3% of citizens do not use cash at all.
- **A Guarantee of Freedom and Independence:** Cash is not only a means of payment but also a symbol of personal freedom and anonymity. Its constitutional protection is now being promoted by the emerging Babiš government, but approval from the Senate will be necessary — and the Senate has not supported the amendment.
- **A Balance Between Both Payment Methods:** The goal should not be the dominance of one form of payment over the other, but balance and the right to choose. Constitutional protection of cash does not mean rejecting digitalization; on the contrary, Czech law should be expanded to include an obligation to accept contactless payments as well.

Introduction

The digitization of identity constitutes one of the most significant developments in European data governance and privacy regulation of the past decade. The European Digital Identity (EUDI) Wallet aims to allow citizens to verify their identity securely and seamlessly across the EU, and is officially framed as a voluntary, privacy-preserving, and user-controlled system.

At the same time, however, the initiative raises a fundamental governance question: whether the digitalization of identity could become a gateway to the broader digitization of civic life, with growing potential for centralized oversight and control. The UK's experience with the proposed BritCard demonstrates how initiatives launched as administrative modernization projects can evolve into tools of surveillance and enforcement.

This analysis argues that the European digital identity framework is not merely a technical infrastructure, but a political project with the potential to reshape the relationship between citizens and the state. Whether the EUDI Wallet ultimately enhances individual autonomy or moves toward a more restrictive model remains an open and critical policy question.

Digital Identity in the EU: Origins, Principles, and Legislative Framework

The introduction of a unified digital identity system, the EUDI Wallet, represents one of the EU's most ambitious recent initiatives. The objective is to create a framework that enables citizens to verify their identity securely and to sign documents online across EU member states. The EUDI Wallet builds upon the eIDAS Regulation (Electronic Identification, Authentication and Trust Services) adopted in 2014, which established the original legal framework for electronic identification and trust services in the EU. In 2024, this framework was significantly revised. The updated regulation, commonly referred to as *eIDAS 2.0*, introduces the concept of a European digital wallet: a user-facing application that allows individuals to store digital identity credentials, qualified electronic signatures, and access data for public and private sector services (EU 2024/1183; Kaminaris 2024).

In its justification for the proposal, the European Commission identifies the primary objective as strengthening security, trust, and user convenience in the digital environment. According to the European Commission, "digital wallets" would operate as a mobile application (or other user application) in which a citizen stores digital documents (e.g., an electronic identity card, driver's license, education certificates, tax returns) and to access public administration services and commercial providers in any Member State.

The European Commission identifies a wide range of practical uses for the electronic wallet. These include applying for a passport or driving license, filing tax returns, opening a bank account, registering a SIM card, signing contracts, collecting prescription medication from a pharmacy, verifying identity for online payments, providing proof of educational qualifications, and accessing social benefits. The system is expected to be fully operational by the end of 2026 and available to all EU Member States' citizens who choose to use a digital identity. Unlike existing national electronic identity systems, the EUDI Wallet is intended to provide seamless, Union-wide interoperability. For example, a citizen registered in the Czech Republic would be able to verify their identity in Germany or France, and vice versa (European Digital Identity 2025).

From a legal perspective, *eIDAS 2.0* seeks to balance two core objectives: privacy protection and reliable identification. A central feature of the framework is the "minimum disclosure" principle,

under which users control which data points they share (e.g., age verification) without revealing their full personal data. On the technological side, the European Commission states that the digital wallet will be developed as an open-source solution with robust cryptographic safeguards, including protections against unauthorized access and data manipulation. From an economic standpoint, the initiative is also presented as efficiency-enhancing. The Commission estimates that full interoperability of digital identities across the EU could generate substantial savings by reducing administrative burdens, accelerating verification procedures, and lowering data management costs (EU 2024/1183).

The End of Anonymity? Digital Identity and Individual Freedom

Online anonymity has long been a key safeguard of freedom in the digital space; it allows individuals to express opinions, share experiences, criticize those in power, and organize without fear of retaliation, social sanction, or reputational harm. The introduction of a unified digital identity for EU citizens raises a fundamental governance question: whether the widespread deployment of digital identity infrastructure could gradually erode anonymity and the civil liberties on which it depends.

According to the official narrative, the digital wallet initiative is intended to make citizens' lives easier: to enable their secure identity verification and allow them to digitally sign documents. Participation is also formally presented as voluntary. However, this claim warrants caution, given the European Commission's long-standing tendency to expand policy initiatives over time. One example is the Green Agenda, where an initial commitment to environmental protection and emissions reduction under the European Green Deal later evolved into far more concrete regulatory measures, such as emissions obligations affecting households and personal transport under Fit for 55. Similarly, serious concerns about mass surveillance were raised during the debate surrounding Chat Control: proposals to monitor communications on private messaging platforms were officially justified as measures to protect children from sexual exploitation (iDnes 2025).

The gradual expansion of policy scope—known as the “salami method”—is a familiar governance dynamic: initial, well-intentioned declarations about protection or public benefit are followed by incremental changes that ultimately reshape the initiative's original purpose. From this perspective, skepticism regarding the true purpose of digital identity initiatives seems warranted.

Digital identity systems can be viewed as a gateway to electronic profiling of citizens. If digital identity is linked to multiple domains—from banking to social media networking and e-commerce—it enables the creation of comprehensive data profiles that can reveal individuals' behavior, preferences, and opinions of any given user. Because digital identity is intended for use in commercial settings, including access to banking, insurance, and social services, private providers may begin to require its use as a condition of access, which can generate pressure toward universal adoption. In other words, an ostensibly voluntary system may, through incremental development and structural pressure, evolve into a de facto mandatory framework with near-universal participation.

A particularly sensitive issue is the linking of digital wallets to private platforms, such as social networks or online marketplaces. This would likely result in an erosion of online anonymity. For example, if access to a social media account or e-commerce services were made conditional on identity verification through a digital wallet, every login, comment, or transaction would be directly attributable to a specific individual. An infrastructure of this nature would create unprecedented opportunities for tracking and profiling user behavior, not only by private companies but also by state institutions. A first step in this direction is the push to introduce age verification requirements for access to social media platforms (European Parliament 2025; Gkritsi 2024). Such verification may rely on bank-based digital identities, or biometric data such as facial images, or other forms of identity confirmation. As a result, individuals could face situations in which creating an email account or accessing social media services is no longer possible without identity verification through official documents or biometric identification, such as submitting an ID card or a facial image (Fišer; Zoulová 2025).

When viewed alongside other EU initiatives—such as the introduction of a digital euro or efforts to measure individual carbon footprints—the concern that digital identity systems could be used to monitor and control citizens’ behavior becomes increasingly credible. Debates surrounding sustainable consumption behavior suggest that personal data could be used to establish individual limits or to impose targeted charges on certain activities. If a digital wallet were to also incorporate payment functions with digital currency, it could evolve into a single access point for multiple dimensions of everyday life (e.g., identity verification, financial transactions, consumer behavior).

Under such conditions, comprehensive digital footprints could be created for individuals, which, at a minimum, enable highly personalized advertisement targeting and, at a maximum, facilitate blanket surveillance and behavioral steering aligned with Brussels’ political or economic priorities. Such a development would significantly constrict the space for anonymous expression and free participation in digital environments, which would erode personal freedom and undermine core civil liberties.

The risks extend beyond these potential threats to individual freedom and anonymity. Any system that centralizes personal data inevitably increases exposure to misuse and security breaches. An attack on digital identity infrastructure could disrupt essential services and generate significant economic and social harm. Moreover, the principle of “minimum disclosure,” frequently emphasized by the European Commission, may sound compelling in theory but offers only partial reassurance, as it fails to fully address how to prevent secondary use of data once it has been shared.

BritCard in the Footsteps of Orwell

The development of digital identity policy in the UK exemplifies the potential consequences of introducing centralized digital identification systems without sufficient safeguards. In 2025, the British government announced plans to implement a mandatory digital identity for all adult workers: the “BritCard.” The stated objective is to ensure that every employee has a verified digital identity by 2029, a tool to combat illegal migration. Under the proposal, access to lawful employment is conditional on possessing a BritCard (Reuters 2025).

The proposal has elicited a strong public response: a petition, *Do Not Introduce Digital ID Cards*, which calls on the UK government to halt plans for mandatory digital identity, gathered approximately three million signatures by November 2025—far exceeding the 100,000-signature threshold required for formal consideration by the UK Parliament.

The petitioners emphasize that no individual should be forced to register in a state-controlled identity system, describing the proposal as a step toward mass surveillance and digital control (Do Not Introduce Digital ID Cards 2025). The tone and scope of the public opposition suggest that the BritCard initiative has struck a sensitive nerve in British society—namely, the issues of freedom, privacy, and the appropriate limits of state authority.

The UK has a long history of public resistance to any form of state registration of citizens. Identity cards were abolished after World War II, and any subsequent attempts to reintroduce them have consistently met strong public opposition. Despite this historical tradition, Keir Starmer’s government has announced plans to make digital identity mandatory for all adult workers by the end of the current election term. Under the proposal, the digital identity would be stored on smartphones and used primarily for employment verification. However, there is already public debate over whether digital identity could also become required in other contexts, including access to National Health Service (NHS) care, applying for social benefits, housing rentals, opening bank accounts, accessing tax records, or obtaining a driver’s license.

Critics argue that a single digital identifier would grant the state access to personal data while also enabling greater state control over access to essential public services and resources. Such a system

risks transforming the UK into a “database state,” where interactions with public authorities or private actors would leave a digital footprint. Those in opposition further warn that mandatory digital identity systems could reverse a core principle of liberal democracy: rather than citizens exercising oversight over the state, the state would acquire enhanced capacity to control citizens.

Experts also caution that the project may fail to deliver its stated benefits in terms of security, migration control, or administrative efficiency. They argue that instead, it could increase burdens on ordinary citizens and exacerbate digital exclusion. Older individuals, socially disadvantaged groups, and those less equipped with digital skills may face increased barriers to accessing essential services. Additionally, a centralized digital identity system would present an attractive target for cyberattacks, heightening the risk of large-scale data breaches. Beyond these technical concerns, critics’ most significant warning is that the UK could evolve into what has been described as “Checkpoint Britain”—a country with “internal borders,” where people would have to constantly prove their identity every time they interact with public authorities, healthcare providers, or financial institutions. Such a framework, critics argue, would lead to pervasive monitoring and profiling, and could erode civil liberties that are the basis of Britain's democratic tradition (Checkpoint Britain 2025).

The British Scenario as a Warning

At present, the distinction between the UK’s BritCard proposal and the European Digital Identity Wallet is substantial. The EU model is presented as a user-controlled system that allows individuals to store identity documents, certificates, and electronic signatures, and to determine which data are shared and with whom. In principle, users would disclose only the minimum information required for a specific transaction—for example, proof of age—without revealing their full personal profile. The project explicitly invokes the principles of privacy by design and voluntariness, positioning it as fundamentally different from the mandatory, state-managed British approach. On paper, these European design choices mark a clear departure from the BritCard model.

By contrast, the BritCard proposal reflects a fundamentally different approach. Rather than serving primarily as a convenience tool for citizens, it is designed as a state-administered system focused on workforce monitoring and employment enforcement. The system is mandatory, centrally managed, and focused on ensuring the legality of employment. By tying legal identity verification directly to labor and immigration policy, the model effectively makes state oversight a precondition for exercising basic rights—such as the right to work, reside, or access services.

The European project is moving in a different direction, in part due to the findings of the SOTERIA study, which tested a digital wallet design emphasizing security, strong encryption, and minimal data disclosure. However, the results indicate that voluntary uptake of such systems remains limited and tends to increase only when use becomes mandatory. This trend creates a structural risk that the EU could follow a trajectory like the one currently unfolding in the UK, in which a voluntary framework gradually shifts toward mandatory implementation, and a model centered on individual autonomy becomes increasingly defined by oversight and control (Das 2025).

Although the EU currently promotes a liberal and decentralized model, growing pressure to ensure “effective interoperability” and to integrate digital identity across public and private services could gradually push the system dangerously close toward a model that closely resembles the UK’s. Once a digital wallet becomes a condition for accessing services, making payments, or communicating with public authorities, it effectively becomes mandatory and, as such, a potential instrument of widespread surveillance. In this sense, the British experience may serve as an early warning for the European Union. A project initially framed around convenience and user empowerment could evolve into a system of control, in which routine activities (e.g., accessing accounts, engaging with public institutions, making purchases) are systematically linked to a verified identity. What is presented today as a tool of modern digital governance could, without robust safeguards, become a permanent infrastructure of surveillance tomorrow: a “Checkpoint Europe.”

Conclusion

The European digital identity framework is currently presented as a voluntary, secure, and citizen-centered system. However, it carries risks similar to those of the British BritCard proposal. Initiatives that begin with technical measures for addressing illegal migration can gradually transform into a mechanism of blanket control, which would produce new forms of social exclusion based on access to services.

At the present moment, the European digital wallet is grounded in the principles of “privacy by design” and “minimum disclosure”; but, its potential integration across commercial and public-sector systems could erode these safeguards over the long-term. Once the use of the wallet becomes a prerequisite for employment, financial transactions, or interaction with public authorities, citizens would lose their freedom of choice. A system originally presented as voluntary could evolve into a mandatory digital gateway governing multiple dimensions of daily life—from identity and finances to patterns of consumption and, perhaps even political opinions.

BritCard, therefore, serves not only as a warning but also as a potential mirror of the European project’s future trajectory. The central question is whether the EU can sustain a balance between technological innovation and the protection of individual freedom, or whether the digital wallet will become an instrument of surveillance and centralized authority.

Sources

- Das, R. 2025, 9. 10. „The UK’s mandatory digital ID scheme is repeating the EU’s mistakes“. LSE EUROPP Blog. Dostupné na: <https://blogs.lse.ac.uk/euoppblog/2025/10/09/britcard-uk-digital-id-scheme-eu-mistakes-identity-wallet>
- Do not introduce Digital ID cards. 2025. Petitions. UK Government and Parliament. Dostupné na: <https://petition.parliament.uk/petitions/730194>
- Evropská digitální identita. 2025. Evropská komise. Dostupné na: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs
- EU 2024/1183. „Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu“. EUR-Lex. Dostupné na: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32024R1183>
- Evropský parlament. 2025, 16.10. „New EU measures needed to make online services safer for minors“. Evropský parlament. Dostupné na: <https://www.europarl.europa.eu/news/en/press-room/20251013IPR30892/new-eu-measures-needed-to-make-online-services-safer-for-minors>
- Checkpoint Britain. 2025. „Checkpoint Britain: The dangers of digital ID and why privacy must be protected“. Big Brother Watch. Dostupné na: <https://bigbrotherwatch.org.uk/wp-content/uploads/2025/09/Checkpoint-Britain.pdf>
- Gkritsi, E. 2024, 3. 10. „European authorities press on with digital wallets for social media, age verification and more“. Euractiv.com. Dostupné na: <https://www.euractiv.com/news/european-authorities-press-on-with-digital-wallets-for-social-media-age-verification>
- iDnes. 2025, 14. 10. „V EU ustoupili od „šmírovací“ směrnice, Dánové se ale návrhu nechtějí vzdát“. iDnes.cz. Dostupné na: https://www.idnes.cz/zpravy/domaci/evropska-komise-unie-chat-control-legislativa.A251014_152811_domaci_tty
- Kaminaris, S. 2024. „Regulation (EU) 2024/1183 – The New Framework for a European Digital Identity.“ EY.com. Dostupné na: https://www.ey.com/en_gr/technical/tax/tax-alerts/ey-regulation-eu-2024-1183-the-new-framework-for-a-european-digital-identity
- Fišer, M., Zoulová, L. 2025. 16. 11. „Občanku nebo sken obličeje. EU má na stole neuvěřitelně invazivní návrh na kontrolu komunikace“. Novinky.cz. Dostupné na: <https://www.novinky.cz/clanek/internet-a-pc-smirovani-komunikace-chat-control-je-zpatky-eu-ma-na-stole-jeste-invazivnejsi-podobu-40549090>
- Reuters. 2025, 26. 9. „Britain to introduce mandatory digital ID cards.“ Reuters. Dostupné na: <https://www.reuters.com/world/uk/britain-introduce-mandatory-digital-id-cards-2025-09-26/>

Author



JAN ROVENSKÝ

Analyst

He graduated from the Faculty of Arts of Charles University, majoring in English and Political Science, and in 2008 he received his PhD in Political Theory from the LUISS Guido Carli University in Rome. For fifteen years he worked at the daily Právo, where he first worked in the foreign editorial office. Since 2009 he has worked in the political department, from 2018 to January 2021 as deputy editor-in-chief. Since February 2021, he has been the media advisor to the chairman of the ANO movement.

Publisher



INSTITUTE FOR POLITICS AND SOCIETY

The institute's mission is to improve the quality of the Czech political and public environment through professional and open discussion and the creation of a lively platform that names major problems, develops their analysis and offers recipes for their solution through the cooperation of experts and politicians, international conferences, seminars, public discussions, political and social analyses available to the entire Czech society. We are convinced that open expert discussion and understanding of the nature and causes of individual problems are a prerequisite for any successful solution to the problems of contemporary society.



Martinská 2, 110 00 Praha 1



+420 602 502 674



www.politikaspolecnost.cz



office@politikaspolecnost.cz