

From Innovation to Inclusion? The Human Rights Dilemma of Digital Citizenship

*Sílvia de Carvalho Homem**

JusGov - Justice and Governance Research Centre, University of Minho Law School, Portugal

Abstract. The development of digital identity systems, driven by biometric technologies, blockchain, and artificial intelligence, has been presented as a tool for security, innovation, and efficiency in public and private services. Yet, their rapid implementation raises critical concerns regarding privacy, data protection, and non-discrimination. The centralization of sensitive data and the interconnection of state and corporate databases create risks of expanded surveillance and exclusion of vulnerable groups. This paper examines the construction of digital citizenship in the European Union, with particular attention to the European Digital Identity Wallet, reflecting on its implications for social justice and democratic participation. The study is grounded in a legal and philosophical framework, integrating insights from human rights law, critical technology studies, and social studies of innovation. It argues that, while digital citizenship is conceived as a vector of inclusion, it risks becoming a mechanism of inequality and control if robust safeguards are not implemented. The analysis underscores the need for public policies that guarantee transparency, proportionality, and independent oversight. It further suggests that digital citizenship should not be reduced to a technological instrument but reimaged as a space for emancipation and democratic participation, where human dignity remains the guiding principle.

1 Introduction: Context and Problematic

Contemporary societies are experiencing a profound transformation driven by the digitalisation of social, economic, and political life. Over recent decades, technological innovation has redefined how individuals interact with states, markets, and institutions. In this context, digital identity has emerged as a central infrastructure of citizenship, mediating access to rights, services, and democratic participation. The ability to authenticate, verify, and transact online has become a precondition for exercising fundamental rights and fulfilling civic duties.

Worldwide initiatives illustrate this trend. In the European Union, the proposed European Digital Identity Wallet (EUDI) aims to provide a harmonised, secure model for identification and authentication across Member States [1]. India's Aadhaar programme (the world's largest biometric ID system) covers more than 1.2 billion residents, while Estonia integrates digital identity into virtually all public interactions, including online voting and cross-border

* Corresponding author: silviadecarvalhohomem@gmail.com

transactions. Despite their differences, these models converge on the understanding that digital identity is now essential to modern citizenship [2].

Policymakers present digital identity as a tool for innovation, efficiency, and inclusion. Advocates highlight its potential to reduce bureaucracy, strengthen trust in digital services, facilitate mobility, and support democratic participation. The European Commission frames the EUDI as part of a “Digital Decade,” aiming for at least 80% of Europeans to use digital identity by 2030 [3].

Yet this promise is accompanied by a fundamental dilemma. Technologies intended to empower citizens may simultaneously enable surveillance, exclusion, and indirect discrimination. Centralised biometric and personal data systems raise concerns about state overreach, while reliance on private actors introduces risks of commodification. Moreover, infrastructures reflect existing social and political power relations. Aadhaar, despite its inclusive aims, has been criticised for excluding marginalised populations and enabling unauthorised surveillance [4]. Estonia’s pioneering model, while efficient, has revealed vulnerabilities through significant cyberattacks [2].

The EU positions itself as a global leader in rights-based digital governance, embedding the EUDI within the GDPR and the Charter of Fundamental Rights [1]. However, translating these principles into practice remains challenging. Key questions persist:

- How much control can citizens truly exercise over their data?
- How resilient are identity systems to misuse by states or private actors?
- How can digital identity avoid reproducing inequalities linked to limited digital access or literacy?

This article addresses these questions by critically analysing the legal and political construction of digital citizenship in the EU. It argues that, while digital identity is envisioned as a vehicle for inclusion and empowerment, it risks producing inequality and surveillance unless supported by robust safeguards.

2 Theoretical Framework: Digital Citizenship, Surveillance and Capabilities

This study adopts a multidisciplinary theoretical framework combining insights from critical citizenship studies, surveillance studies, biopolitics, and the capability approach. Together, these perspectives clarify how digital identity systems shape contemporary forms of belonging, participation, and inequality.

First, digital citizenship is understood through the work of Isin and Ruppert, who argue that citizenship is not merely a legal status but a set of practices enacted through digital infrastructures. Identification, authentication, and data disclosure become central acts through which political subjectivity is produced online. From this perspective, digital identity systems mediate new forms of agency but also condition the terms under which such agency is exercised. Understanding digital citizenship as a performative and technologically mediated practice allows us to examine how tools such as the European Digital Identity Wallet (EUDI) shape rights, obligations, and experiences of inclusion.

Second, the analysis draws on Michel Foucault’s concepts of biopolitics and governmentality. Digital identity functions as a governance technology that regulates populations through the continuous recording, classification, and monitoring of bodies and actions. Power is exercised not through overt coercion but through diffuse mechanisms of surveillance and normalisation. The integration of data across health, finance, and mobility creates infrastructures capable of producing “governable digital subjects,” often under the narrative of efficiency and security.

The framework is further informed by David Lyon’s notion of the culture of surveillance. Lyon argues that surveillance has become a routine aspect of everyday life, embedded in both

public and private systems. Digital identity programmes exemplify this condition: while promising convenience and personalisation, they rely on the constant extraction, circulation, and verification of personal and biometric data. Situating the EUDI within this culture of surveillance illuminates the tension between empowerment and monitoring that characterises contemporary digital governance.

Fourth, Amartya Sen's capability approach highlights that genuine inclusion requires more than formal access to digital tools. Effective participation depends on individuals' real freedoms, including access to devices, connectivity, literacy, and support systems. Without these capabilities, digital identity initiatives risk deepening inequalities and excluding vulnerable groups, even if formally accessible to all.

Anchoring these perspectives is the principle of human dignity, enshrined in the EU Charter of Fundamental Rights. Human dignity provides the normative baseline for evaluating digital identity systems, requiring that individuals retain meaningful autonomy and control over personal data. This principle connects and reinforces the other theoretical dimensions, ensuring that the analysis goes beyond technical issues to address broader ethical and political implications.

Together, the concepts of digital citizenship, biopolitics, surveillance culture, capabilities, and human dignity provide a coherent foundation for analysing the risks and opportunities of digital identity in the EU, highlighting how infrastructures reshape power relations and redefine the boundaries of citizenship in the digital age.

3 The Legal Construction of Digital Citizenship

Building on the theoretical framework outlined above, this section examines how legal and institutional infrastructures materialise digital citizenship and shape the conditions under which individuals exercise rights in the digital environment.

Digital citizenship extends beyond the use of technological tools. It reconfigures classical notions of citizenship—traditionally based on rights and obligations—by incorporating new forms of belonging and participation mediated by electronic platforms. Legal frameworks therefore play a central role in determining how digital identity technologies are embedded within democratic societies, and the European Union has assumed a leading role in this transformation.

The European Digital Identity Wallet (EUDI) is conceived as a mobile application enabling individuals to store and manage personal attributes such as age, nationality, qualifications, health data, and licences. Users may decide which attributes to share in specific interactions, reflecting the GDPR's principle of data minimisation. Designed for both online and offline use, the Wallet intends to function across public and private services and across borders, facilitating actions such as opening a bank account, enrolling in university abroad, or accessing medical records.

Although the Commission emphasises that the EUDI will be voluntary, past experience suggests that digital identity systems often become *de facto* mandatory when linked to essential services. India's Aadhaar system, initially optional, became indispensable for welfare benefits and private services, illustrating the risk of functional compulsion [4]. The EU must therefore address this possibility from the outset.

The European experience does not develop in isolation. Estonia has long been regarded as a pioneer in digital governance: its national ID card and e-residency programme allow near-universal access to public services, tax filing within minutes, and online voting. However, the 2007 cyberattacks revealed the vulnerabilities of hyper-digitalisation, prompting Estonia to create the world's first "data embassy" to protect critical digital assets [2].

Pilot projects launched in Germany and France between 2023 and 2024 explored EUDI applications in education, mobility, and health. Early assessments identified both opportunities and challenges: while cross-border interoperability appears promising, user trust remains fragile, especially regarding sensitive data such as health information.

The Portuguese case illustrates regulatory tensions. In 2024, the company Worldcoin collected iris scans from more than 300,000 citizens in exchange for cryptocurrency. The National Data Protection Authority (CNPD) suspended the project, citing concerns about informed consent, the collection of minors' biometric data, and the lack of mechanisms to erase such records. This episode underscores the risks associated with private-sector-led biometric initiatives and the importance of strong independent regulators [5].

Beyond Europe, comparisons with India's Aadhaar system are instructive. While Aadhaar sought inclusion, the Indian Supreme Court identified privacy violations and the exclusion of vulnerable groups due to biometric errors [4]. This example demonstrates how rapidly digital identity can shift from inclusion to exclusion if embedded within essential service delivery without adequate safeguards.

The EU aims to avoid these pitfalls by embedding rights-based protections into the design of the EUDI. Yet successful implementation will depend on addressing practical challenges related to interoperability, user trust, accountability, and the balance between public interest and individual rights.

4 Human Rights in the Age of Digital Identity

Digital identity systems intersect directly with the European human rights framework, which provides some of the world's strongest protections for personal data. Yet even within this robust legal environment, implementation challenges raise significant concerns regarding privacy, equality, dignity, and democratic participation.

A central risk is the expansion of surveillance. Even when designed with decentralisation in mind, the aggregation of identity attributes across sectors such as health, finance, education, and mobility creates the possibility of detailed cross-sectoral profiling. The logic of interoperability, while enhancing efficiency, amplifies surveillance potential. Foucault's analysis of disciplinary power is instructive here: technologies intended to secure populations may easily be repurposed as instruments of control [6].

The Worldcoin case in Portugal illustrates this dynamic. By exchanging iris scans for cryptocurrency, the company collected a vast biometric database (including minors) without clear guarantees of data erasure or adequate safeguards [5]. Although not an EU initiative, the episode demonstrates how biometric data can be commodified and how vulnerable populations may consent under economic pressure.

Another concern involves the growing use of artificial intelligence (AI) in authentication. Facial recognition, biometric matching, and automated decision-making systems can reproduce structural biases. Studies show higher error rates for women and people with darker skin tones, resulting in discriminatory access outcomes. Although the EU's AI Act (2023) restricts high-risk AI applications (including biometric identification in public spaces) important grey areas remain, especially when AI is embedded in verification processes that affect access to essential services.

Agamben's concept of the "state of exception" is relevant here: emergency-driven data collection may become normalised, allowing extraordinary practices to persist beyond their original justification. This risk became visible during the COVID-19 pandemic, when temporary digital health passes blurred the boundary between public health measures and long-term identity governance.

Inclusion poses a further challenge. As digital identity becomes central to accessing welfare, healthcare, education, and mobility, individuals without digital devices, internet

access, or digital literacy may experience exclusion. Elderly populations, rural communities, and low-income groups are particularly at risk. While inclusion is not explicitly codified as a right in EU law, it is implicit in the broader principles of equality and non-discrimination. The shift toward mandatory or quasi-mandatory digital identity risks transforming a technological design issue into a question of social justice.

Amartya Sen's capability approach provides an essential analytical lens: genuine inclusion depends not only on formal access to tools but also on individuals' effective ability to use them [7]. Thus, the success of the EUDI will rely not only on technical design but also on policies ensuring digital literacy, device access, and targeted support for vulnerable groups. Underlying privacy, equality, and inclusion is the principle of human dignity: the foundational value of the EU Charter. Dignity requires that digital identity systems preserve individual autonomy and prevent the reduction of persons to data objects. This principle demands more than GDPR compliance: it requires transparent governance, meaningful consent, and the prevention of surveillance becoming a "new normal."

David Lyon's concept of the "culture of surveillance" reinforces this concern. Surveillance practices have become embedded in daily life and often accepted as the price of convenience [8]. The EU must therefore resist the normalisation of surveillance logics and ensure that digital identity strengthens rather than undermines the democratic relationship between individuals and institutions.

5 The Inclusion Dilemma: Innovation or Control?

This section analyses the ambivalent nature of digital identity systems through the lenses of surveillance studies and the capability approach, highlighting their dual potential for empowerment and exclusion.

The discourse surrounding digital identity is often highly optimistic. Digital identity is presented as a tool that simplifies administrative procedures, strengthens the security of financial transactions, facilitates cross-border mobility, and supports democratic innovation through digital participation. Within this narrative, the European Digital Identity Wallet (EUDI) embodies the EU's ambition to offer a user-centric and interoperable model that enhances data control and reduces reliance on external technology providers [9].

However, beneath this rhetoric lies a more complex reality. Digital identity technologies operate within a fundamental dilemma: while they may promote inclusion, they also enable new forms of surveillance, exclusion, and social stratification.

The innovation narrative portrays digital identity as a natural extension of modern governance. For instance, the Commission describes the EUDI as a mechanism for empowering individuals to control their personal data and engage seamlessly with public and private services. Similarly, the World Bank's Identification for Development (ID4D) initiative frames digital identity as essential to achieving the Sustainable Development Goals by ensuring legal identity for all by 2030 [3].

The inclusion narrative stresses the potential of digital identity to reduce inequalities, especially in regions where many individuals lack official documentation. In the EU, inclusion is associated with cross-border mobility and equal access to services for mobile citizens. Yet these narratives often conceal structural power asymmetries and the potential risks embedded in digital infrastructures.

India's Aadhaar system illustrates these tensions. Designed as an inclusive initiative, Aadhaar soon became mandatory in practice for access to welfare, subsidies, and private services such as banking. Biometric authentication errors excluded millions, particularly vulnerable individuals. The Indian Supreme Court recognised privacy as a constitutional right in the Puttaswamy judgment (2018) and imposed limits on Aadhaar, but the consequences for public trust were significant [4].

In the EU context, the EUDI is formally voluntary. Yet, if adopted by essential services, it may generate de facto obligation, creating a divide between digitally integrated citizens and those excluded due to technological, economic, or educational barriers.

Exclusion risks also arise from the use of biometric identifiers, such as facial recognition and iris scanning. Studies have shown that biometric systems misidentify women and people with darker skin tones at disproportionately high rates, reproducing systemic inequalities and leading to unjustified denials of access.

A second layer of the dilemma concerns surveillance. The integration of identity attributes across health, finance, and mobility creates the potential for granular profiling. While the EU highlights the decentralised architecture of the EUDI, interoperability across Member States may enable cross-sectoral surveillance.

The EU seeks to differentiate its model from global alternatives. China integrates digital identity with social credit scoring, while in the United States private corporations dominate identity verification. By contrast, the EU promotes a rights-based approach grounded in the GDPR and the Charter of Fundamental Rights.

Nonetheless, challenges remain. Interoperability across Member States with uneven digital infrastructures may produce fragmented implementation. Moreover, although the EUDI emphasises user control, refusal to share attributes may limit access to services, making “consent” illusory. The reliance on private actors in infrastructure development raises concerns about commercial exploitation of identity data.

Ultimately, the inclusion dilemma extends beyond service access to the nature of citizenship itself. As citizenship becomes mediated by digital platforms, exclusion from these systems risks translating into exclusion from civic life. Digital identity systems can therefore entrench digital stratification even as they aim to democratise access.

At the same time, digital identity can enable new forms of democratic participation, such as secure digital voting, deliberation platforms, or cross-border democratic engagement. Yet such innovations require careful governance to prevent surveillance, manipulation, or exclusion.

The EU thus faces a profoundly political choice: whether digital identity will function as an instrument of empowerment and democratic inclusion or evolve into a mechanism of control and inequality. The outcome will depend on governance structures, institutional accountability, and the extent to which citizens' autonomy remains central to digital infrastructures.

6 Safeguards for a Just Digital Citizenship

To ensure that digital identity functions as a tool of inclusion rather than exclusion, robust safeguards are essential. These must extend beyond technical solutions to encompass legal, institutional, and social dimensions. Digital identity systems are never neutral; they reflect political priorities and power structures. The EU therefore faces the challenge of designing a model that strengthens democratic citizenship while protecting fundamental rights.

A first layer of protection lies in the legal framework. The GDPR imposes strict requirements on the processing of personal data, including biometric identifiers. These principles must be fully embedded in the architecture of the EUDI Wallet. Four elements are especially critical:

1. Proportionality – data processing must be strictly limited to what is necessary.
2. Purpose limitation – data collected for one function cannot be reused for another.
3. Privacy by design and by default – systems must be built to minimise data exposure.
4. Accountability – public bodies and private providers must be responsible for misuse, with accessible redress mechanisms for citizens.

From a technical standpoint, several measures are key to ensuring trust and security.

- Decentralised data storage: rather than relying on centralised databases prone to hacking or misuse, identity data should remain under the individual's control. The EUDI's wallet-based model contributes to this aim.
- Strong cybersecurity standards: past incidents, such as the 2007 cyberattacks on Estonia, highlight the need for robust, resilient systems. ENISA will play a crucial role in setting and enforcing standards.
- Algorithmic transparency: when AI or biometric systems are used, they must be explainable and auditable. Black-box models undermine accountability.
- Cautious evaluation of blockchain/DLT: although often praised for transparency, immutability may conflict with rights such as data erasure. Full assessment is required to align these technologies with EU principles.

Even the most sophisticated legal and technical safeguards are insufficient without independent oversight. Institutions such as the European Data Protection Supervisor (EDPS) and national Data Protection Authorities (DPAs) must have adequate resources and authority to monitor digital identity systems. The Portuguese CNPD's intervention in the Worldcoin case demonstrates the importance of strong regulators capable of halting practices that endanger rights [5].

Effective oversight also requires cross-border coordination. Given the EUDI's interoperability, DPAs must work together to prevent regulatory arbitrage: where actors exploit weaker enforcement in some jurisdictions. Common standards, joint investigations, and shared expertise will be vital to ensuring equal protection across all Member States.

At the centre of all safeguards lies human dignity, the cornerstone of the EU's normative framework. Digital identity systems must never reduce individuals to data points, but affirm autonomy, equality, and control. Embedding a culture of accountability is essential: accessible complaint mechanisms, judicial recourse, and transparent decision-making processes help ensure that both public institutions and private actors are held responsible.

Ultimately, safeguards must be understood not as technical add-ons but as democratic commitments essential to building trust. The legitimacy of digital identity depends on transparent governance, robust legal protections, and accountability structures capable of preventing abuse.

7 Conclusion: Rethinking Citizenship in the Digital Age

This analysis shows that the future of digital identity depends not only on technological design but also on the broader political and ethical commitments that shape its implementation. Digital citizenship stands at a pivotal moment. While initiatives such as the European Digital Identity Wallet (EUDI) promise innovation, efficiency, and inclusion, they also raise substantial risks of surveillance, exclusion, and discrimination. The dilemma is therefore not merely technical but profoundly ethical and political.

A key finding is that digital identity cannot be treated as a neutral instrument. It constitutes a political institution that shapes belonging, participation, and rights in contemporary societies. As Isin and Ruppert argue, citizenship is enacted through practices and technologies as much as through legal status [10]. Embedding identity management into digital infrastructures reshapes the boundaries of political community and raises the possibility that exclusion from digital systems may effectively mean exclusion from citizenship itself.

The EU seeks to present a rights-based alternative to global models, contrasting with China's surveillance-driven approach and the United States' market-led systems. Anchoring the EUDI in the GDPR and the Charter of Fundamental Rights reflects this normative ambition. Yet structural vulnerabilities persist, including uneven national infrastructures,

reliance on private providers, and the risk that a formally “voluntary” system becomes indispensable in practice.

The EU’s credibility will depend on translating rights-based principles into concrete safeguards. Central to this is building institutional resilience, fostering citizen trust, and ensuring accountability at all levels. Safeguards such as privacy by design, algorithmic transparency, and independent oversight must be treated as democratic obligations rather than technical features.

Addressing the digital divide remains equally important. Without access to devices, connectivity, and digital literacy, digital identity initiatives may deepen rather than mitigate inequality. In line with Amartya Sen’s capability approach, digital identity systems must expand individuals’ real freedoms and support participation with dignity.

Ultimately, digital citizenship compels a rethinking of what it means to belong and participate in the digital age. Its legitimacy depends on respect for rights, dignity, and inclusion. Without these commitments, digital identity risks becoming a Trojan horse of control rather than a tool of empowerment. The future of citizenship in the digital era will be shaped by decisions made today: whether digital identity becomes a means of emancipation or a mechanism of domination.

References

1. European Commission, European Digital Identity Architecture and Reference Framework (2022). <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>
2. J. Priisalu, R. Ottis, Personal control of privacy and data: Estonian experience, *Health Technol.* 7, 441–451 (2017).
3. European Commission, Europe’s Digital Decade: Digital Targets for 2030 (2021). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
4. Supreme Court of India, Justice K.S. Puttaswamy (Retd.) vs. Union of India (Aadhaar case), 2018. <https://translaw.clpr.org.in/case-law/justice-k-s-puttaswamy-anr-vs-union-of-india-ors-privacy/>
5. CNPD Portugal, Deliberação sobre a suspensão da recolha de dados biométricos pela Worldcoin (2024). https://www.cnpd.pt/media/bzwb5k5j/comunicado-de-imprensa_cnpd-suspende-recolha-de-ddos-da-worldcoin_26-mar%C3%A7o-2024.pdf
6. M. Foucault, *Security, Territory, Population: Lectures at the Collège de France* (Palgrave, 2008).
7. A. Sen, *Development as Freedom* (Oxford University Press, 1999).
8. D. Lyon, *The Culture of Surveillance* (Polity Press, 2018).
9. European Data Protection Supervisor (EDPS), Where are we heading with digital identities? (2023). https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/2023-02-07-where-are-we-heading-digital-identities_en
10. Ruppert, Evelyn & Isin, Engin. (2015). *Being Digital Citizens*. 10.5040/9798881809959.