Observatoire ARGA

ARGA Atlas

DIGITAL IDENTITY AS RISK

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA, ARGA Atlas

Mailing address: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org, https://www.arga-atlas.com/

Anglet, 18 avril 2026

Purpose of the document:

This report is prepared to analyze digital identity not as a neutral technological convenience, but as an autonomous source of legal, procedural and transnational risk. Its practical purpose is to show how a person's digital profile, digital documents, credentials, behavioural traces, linked records, and digital identification and verification infrastructures begin to function as channels of admission, exclusion, suspicion, selection, compliance screening, migration control, law-enforcement attention and broader transnational pressure. For ARGA, this topic has practical significance in cases where the protection of the individual increasingly depends not only on the content of legal documents, but on how that individual's digital trace has already been integrated into decision-making systems before any formal legal dispute begins. OHCHR expressly treats privacy in the digital age as an autonomous human-rights issue, while the European Commission confirms that by the end of 2026 Member States must make European Digital Identity Wallets available to citizens, residents and businesses, which gives the topic direct institutional urgency. (ohchr.org)

CONTENTS

1. Executive Summary

Digital identity no longer concerns only how a person proves who they are online. In the contemporary institutional environment, it is becoming a complex system of data, attributes, verifiable signals, behavioural traces and relational links through which state bodies, financial institutions, platforms, employers, migration services and law-enforcement structures obtain the ability not only to recognize the person, but to form a preliminary judgment about that person. OHCHR treats the digital environment as a domain directly affecting a wide range of human rights, not merely issues of technical data security. (ohchr.org)

The practical risk lies in the fact that digital identity begins to function as an instrument of anticipatory judgment. A person is increasingly evaluated through a bundle of digital traces, documents, social links, travel histories, records of interaction with systems and other identity-linked datasets. OHCHR's 2025 paper on AI and counter-terrorism expressly warns that state systems may aggregate and analyse highly personal or sensitive data, including travel information, criminal records, family and social associations and other datasets of personal information. As a result, digital identity turns from a technical function into an infrastructure of legal risk. (ohchr.org)

The importance of the topic is intensified by the fact that digital identity is being institutionalized in Europe and beyond as a normal part of access to services and legally relevant acts. The European Commission confirms that European Digital Identity Wallets must become available by the end of 2026, while the EDPS in TechDispatch 3/2025 specifically identifies privacy risks associated with such wallets. This means that the issue is not a rare or experimental technology, but a normatively supported direction of development in which convenience, verification and legal risk all expand together. (commission.europa.eu, edps.europa.eu)

2. Context & Problem Statement / Why This Topic Has Legal and International Significance

Digital identity has international significance because a growing share of legal and social access is mediated through digital infrastructures. The person is increasingly authenticated not only by passport or physical presence, but through digital documents, wallets, eID, account-based verification, interoperable credentials and other mechanisms that can easily be connected to public and private systems. The European Commission expressly describes the EUDI Wallet as a means of access to public and private services, storage and sharing of digital documents, and the use of legally significant signatures. (commission.europa.eu)

From a human-rights perspective, the problem is that digital identity creates a new layer of preliminary normative reality. A person first passes through systems of digital recognition, correlation and assessment, and only afterwards gains the opportunity to interact formally with an institution. OHCHR's work on digital space and human rights makes clear that technological arrangements may affect privacy, freedom of expression, non-discrimination, security and access to protection. This means that digital identity must be analyzed not as a narrow convenience issue, but as a legal environment in which trust and suspicion are pre-allocated. (ohchr.org)

In transnational matters, this risk is especially visible. A person's digital profile may influence visa decisions, migration control, banking compliance, employer screening, platform verification, police data matching, travel-risk assessments and related processes. In 2026, OHCHR separately called for inputs on the protection of human rights defenders in the digital age, explicitly noting that new and emerging technologies create specific threats for defenders and other vulnerable actors. Digital identity therefore becomes not a secondary topic, but part of the architecture of contemporary transnational pressure. (ohchr.org)

3. Legal Framework / Normative and Institutional Framework

The first layer of the normative framework consists of international standards on human rights in the digital environment. OHCHR maintains dedicated workstreams on privacy in the digital age and digital space and human rights, which in itself confirms that digital technologies and digital personhood are treated as direct human-rights issues. This matters because digital identity cannot be reduced to cyber-security or technical regulation. It is linked to autonomy, surveillance, error, secondary use of data and effective access to protection. (ohchr.org, ohchr.org)

The second layer is the European framework of data protection and informational self-determination. The Council of Europe, in its Digital Development and Governance Focus 2024–2025, explicitly stresses the importance of the right to data protection and informational self-determination, including through Convention 108. For digital identity, this is fundamental because the issue concerns not only storage of data, but the right of the individual to retain meaningful control over how data about them are structured, linked, circulated and reused. (coe.int)

The third layer is the evolving EU legal architecture on digital identity. The European Commission states that the European Digital Identity Regulation provides the legal basis for EUDI Wallets and that by the end of 2026 wallets are to be made available in all Member States. The Commission also explains that the new model is built on existing national digital identities and expands their usability across services. This means institutional normalization of digital identity as a support structure for significant legal and quasi-legal acts. (ec.europa.eu, commission.europa.eu)

The fourth layer is supervisory and privacy-risk guidance. The EDPS, in TechDispatch 3/2025, specifically examines digital identity wallets as an environment with distinct privacy risks, while EDPB materials show that eIDAS, digital identity and adjacent data-processing frameworks are under active regulatory scrutiny. Even if these materials do not provide an exhaustive universal rights doctrine, they confirm that supervisory authorities themselves treat digital identity as a normatively sensitive infrastructure rather than a neutral technological tool. (edps.europa.eu, edpb.europa.eu)

4. Mechanisms of Practice / Abuse / Key Mechanisms of Practice, Abuse, or Conflict

The first risk mechanism is aggregation. Digital identity becomes dangerous not when a single identifier exists, but when multiple streams of data become linkable. Official credentials, platform activity, travel records, social graph signals, employment traces and policing-adjacent information begin to form a composite picture of the person. OHCHR's AI and counter-terrorism paper expressly warns about the aggregation of highly personal and sensitive data by state systems. (ohchr.org)

The second mechanism is portability and reusability. Once identity-linked information is translated into standardized digital formats, it becomes easier to reuse across multiple institutional environments. The European Commission expressly notes that the EUDI Wallet is designed for storage and sharing of documents, access to services and use in both public and private sectors. This increases convenience, but at the same time means that the same digital representation of the person may influence multiple decisions across different sectors. (commission.europa.eu)

The third mechanism is inferential expansion. A system created for authentication may gradually begin to support inferences about reliability, risk, status, trust or suspicion. The EDPS identifies privacy risks in digital identity wallets, while OHCHR's AI and counter-terrorism materials show how aggregated datasets can feed analysis and decision-making by state authorities. The legal danger lies in the fact that the person may formally agree to one layer of data use without realizing the scale of the inferential layering that develops around it. (edps.europa.eu, ohchr.org)

The fourth mechanism is transnational replicability. The more compatible and mutually recognized digital identity frameworks become, the faster signals attached to a person's profile begin to affect different jurisdictions and sectors. The EU digital identity framework expressly pursues cross-border

usability and trust architecture. In sensitive files, this means that a digital identity risk rarely remains local once the infrastructures are interoperable. (digital-strategy.ec.europa.eu)

5. Case Patterns / Typical Scenarios, Patterns of Development, or Practice Models

The first typical scenario is unexplained screening friction. A person encounters verification delays, enhanced due diligence, refusal of service, mobility difficulties or other friction-like treatment while no explicit adverse legal act is visible. In such situations, digital identity may function as the silent carrier of aggregated signals used for filtering or suspicion. OHCHR's privacy and digital-rights framework, together with EDPS concern about wallet-related privacy risks, makes this scenario legally intelligible even where the exact data chain remains difficult to see. (ohchr.org, edps.europa.eu)

The second scenario is the use of a digital profile as a channel for targeting defenders, journalists or politically exposed persons. OHCHR's 2026 call for inputs on the protection of human rights defenders in the digital age expressly confirms that new and emerging technologies create specific risks for such subjects. In these cases, digital identity ceases to be a neutral verification mechanism and becomes a channel of observation, mapping of contacts, vulnerability exposure or pressure. (ohchr.org)

The third scenario is the gradual expansion of the role of identity wallets beyond authentication. A wallet may initially be perceived as a convenient repository and identity-confirmation instrument. But the Commission explicitly describes it as a means of storing documents, accessing services, using signatures and interacting with both public and private counterparties. Around it there therefore gradually forms a legally significant infrastructure whose failures or biases may affect multiple rights-relevant interactions at once. (commission.europa.eu)

The fourth scenario is AI-assisted overlay on identity-rich datasets. OHCHR's 2025 paper on AI and counter-terrorism directly shows that state systems may use combined datasets including social networks, criminal records, travel information and other personal data. When such analytics are layered over digital identity, the person becomes an object not only of recognition but of probabilistic assessment that may be materially consequential and weakly contestable. (ohchr.org)

6. Risk Assessment / Main Risks, Legal Vulnerabilities, and Problem Areas

The first risk is visibility without contestability. Digital identity makes the person more visible to systems, but does not necessarily grant them a proportionate ability to understand, verify or challenge the inferences made about them. OHCHR's work on privacy in the digital age reflects precisely this structural tension between growing institutional knowledge and shrinking individual control. (ohchr.org)

The second risk is function creep. A system introduced for authentication begins to serve tracking, profiling, risk scoring, exclusion or secondary-use logics. The EDPS gives separate attention to the privacy risks of digital identity wallets precisely because the danger lies not only in data breach, but in architectural expansion of use. (edps.europa.eu)

The third risk is cross-sector spillover. The same identity-linked signal may begin to operate simultaneously in banking, migration, employment, platform or law-enforcement contexts. The Commission itself describes the wallet as usable across public and private services, confirming the broad operational footprint of such a profile. (commission.europa.eu)

The fourth risk is asymmetry in transnational contexts. States and large institutions can rapidly correlate identity-related data and signals, while the affected person often cannot reconstruct the chain

of use or inference. OHCHR's AI and digital-rights materials confirm that digital technologies can intensify existing rights vulnerabilities, especially in contexts of state interest, security or political sensitivity. (ohchr.org)

7. Institutional Gaps / Institutional Limitations, Gaps, Deficits of Safeguards, or Systemic Weaknesses

The first systemic weakness is legal normalization outpacing remedial clarity. The EU is actively building the legal basis and implementation environment for digital identity wallets, yet the practical pathways through which individuals can understand, challenge and limit downstream harms are less visible than the architecture of rollout itself. When infrastructure expands faster than clear avenues of contestation, law creates convenience before it secures recourse. (ec.europa.eu)

The second weakness is an excessively narrow privacy framing. Data protection is crucial, and both the Council of Europe and EU supervisory bodies emphasize it consistently. But digital identity as risk also concerns freedom of movement, equality, due process, profiling, exclusion and transnational targeting. If the issue is treated only as a privacy-compliance matter, broader rights harms can remain under-analysed. (coe.int)

The third weakness is fragmentation of oversight. Different parts of the problem are distributed between privacy regulators, courts, migration authorities, police bodies, platforms, banks and human-rights mechanisms. As a result, the same risk may be visible to everyone in fragments and to no one in full. Council of Europe and OHCHR materials are important precisely because they enable one to see digital identity not as a siloed technical issue, but as a cross-rights governance problem. (coe.int, ohchr.org)

8. Practical Guidance / Practical Recommendations and Model of Legal Action

The first step is to treat digital identity as an evidentiary environment. In every sensitive case, counsel should ask which digital representations of the person may already be affecting institutional behaviour: official eID use, wallet-linked credentials, searchable traces, prior screening outcomes, linked social or travel data. Without this, the defense risks contesting only the visible act while ignoring the digital environment that prepared it. (commission.europa.eu)

The second step is to map identity-linked risk across sectors. The same digital profile may matter differently for a border authority, bank, platform, employer or court. Practical defense therefore requires a matrix: where the data circulate, who relies on them, for what purpose, and with what potential harm. Materials of the Commission and EDPS confirm the inherently multi-service nature of digital identity infrastructures. (commission.europa.eu, edps.europa.eu)

The third step is to insist on minimization, selective disclosure and challengeability. Wherever digital identity systems are used, the legal strategy should favour architectures and practices that reduce unnecessary exposure of data, limit secondary use and preserve the ability to contest adverse inferences. This directly accords with the logic of Council of Europe data-protection standards and EU supervisory concern about privacy-by-design. (coe.int, edps.europa.eu)

The fourth step is to integrate digital identity into human-rights and transnational-repression analysis. In politically sensitive, extradition-sensitive or defender-sensitive cases, the digital profile should be treated as part of the core protection file, not as an IT annex. Current OHCHR materials on defenders in the digital age and on AI and surveillance risks directly support such integration. (ohchr.org, ohchr.org)

9. Policy Recommendations / Recommendations on Legal and Institutional Approach

First, digital identity governance should be built around rights-preserving architecture rather than adoption metrics alone. Rollout without strong contestability, minimization and clear limits on downstream use risks turning convenience infrastructure into rights-risk infrastructure. EU and supervisory materials already point in this direction, but they should be read more broadly as protection-by-design rather than privacy-by-design alone. (commission.europa.eu, edps.europa.eu)

Second, policymakers should explicitly address the intersection between digital identity, surveillance, AI and transnational risk. OHCHR's 2025–2026 work demonstrates that these domains are already connected in human-rights analysis. To treat them as separate policy silos is simply a bureaucratic way of making life easier for the risk itself. (ohchr.org, ohchr.org)

Third, legal practice should adopt a digital-identity-as-risk doctrine for sensitive cross-border files. Such a doctrine should proceed from the premise that a person may be judged, filtered or constrained through digital representations long before any explicit legal act becomes contestable. For ARGA, this is particularly important as part of a modern defensive model that does not wait for final formal injury in order to recognize pre-formal digital vulnerability. (ohchr.org)

10. Conclusion

Digital identity has ceased to be merely a convenience layer attached to legal life. It is becoming one of the infrastructures through which legal life is organized, filtered and acted upon. OHCHR, the Council of Europe, the European Commission, the EDPS and related supervisory materials all confirm, from different angles, the same core reality: digital identity systems may increase usability and trust, but they also generate concentration of information, traceability, privacy risk, inferential exposure and cross-sector consequences. (ohchr.org, commission.europa.eu)

For ARGA, the central conclusion is that in contemporary sensitive cases the digital profile must be protected no less seriously than the paper case file, testimony or international legal status. When institutions increasingly see the person through digital identity first, a defense that ignores that identity begins arguing only after a substantial part of the decision has already been silently shaped by the system. An unpleasant evolution, but a very officially organized one. (ohchr.org)

11. Appendix A. Terminology

Digital identity. The aggregate of digital means, data and identifiers through which a person is authenticated, described, verified and recognized in digital and institutional systems. In the current legal context, this includes both official eID components and the broader set of data-linked representations of the person. (commission.europa.eu)

Digital Identity Wallet. A digital wallet enabling a user to prove identity, access services, store and share digital documents, and use legally significant credentials and signatures. In the EU, this tool is embedded in the European Digital Identity framework. (commission.europa.eu)

Informational self-determination. The right and ability of an individual to retain meaningful control over the collection and use of data about themselves. The Council of Europe explicitly links digital governance with this concept. (coe.int)

Function creep. The gradual expansion of identity-related systems beyond their initially declared purpose, for example from authentication to profiling, monitoring or exclusion. This risk is normatively consistent with the EDPS analysis of privacy risks in digital identity wallets. (edps.europa.eu)

Identity-linked inference. Conclusions about the person formed on the basis of aggregated or correlated digital data rather than direct explicit proof. OHCHR's AI materials confirm the reality of this risk. (ohchr.org)

12. Appendix B. Risk / Powers / Legal Consequences Matrix

Task	**Legal risk**	**Legal limit**	**Possible consequence**	**Practical comment**
Treat digital identity as merely technical background	Underestimation of the legal significance of aggregation	Digital identity affects rights, access and institutional treatment	The source of screening or exclusion remains unseen	Begin sensitive cases with identity-environment mapping
Treat wallet/eID as neutral convenience	Function creep and secondary use	Identity systems must remain rights-constrained	Profiling, traceability, institutional overreach	Demand minimization and purpose limitation
Ignore cross-sector use of identity-linked data	Fragmented defense	Public and private services may rely on the same infrastructure	Banking, mobility, employment or reputational spillover	Map all sectors touched by the digital profile
Treat privacy as the only issue	Excessively narrow legal framing	Broader rights such as equality, due process and movement may be implicated	Loss of major lines of argument	Frame the issue as a multi-rights problem
Ignore AI/surveillance overlay	Hidden inferential escalation	Identity-rich data can feed automated decisions	Risk scoring or targeting with weak contestability	Look for inferential uses, not only raw records
Wait for an explicit formal injury	Late recognition of digital risk	Many harms emerge pre-formally	Missed window of preventive protection	Protect the profile before the final adverse act

This matrix reflects recurring risk logic emerging from OHCHR, Council of Europe, Commission and supervisory materials on digital identity, privacy and digital governance. (ohchr.org)

13. Official Sources

- OHCHR, Privacy in the Digital Age. The main official source confirming that the digital environment and data processing are direct human-rights issues rather than merely technical regulation. (ohchr.org)
- OHCHR, Digital Space and Human Rights. Important as a broader human-rights context for the digital environment. (ohchr.org)
- OHCHR, 2026 Call for Inputs on the protection of human rights defenders in the digital age. A current source confirming that new digital technologies are officially treated as risk-generating for defenders and other vulnerable actors. (ohchr.org)

- Council of Europe, Digital Development and Governance Focus 2024–2025. Significant for linking the topic to data protection and informational self-determination within the European human-rights architecture. (coe.int)

- European Commission, European Digital Identity pages and EUDI Regulation materials. The key current sources on the legal basis, functions and rollout logic of EU Digital Identity Wallets, including the target date of end-2026 availability. (commission.europa.eu, ec.europa.eu)

- European Commission, FAQ on the European Digital Identity Framework. Useful for the operational and technical framing of the wallet ecosystem. (ec.europa.eu)

- EDPS, TechDispatch #3/2025 on Digital Identity Wallets. Particularly important as a supervisory document focused on privacy risks associated with digital identity wallets. (edps.europa.eu)

- OHCHR, 2025 position paper on AI and counter-terrorism. Important for showing how identity-rich datasets can be aggregated and analysed by state authorities in ways that materially affect rights. (ohchr.org)