

Digital Identity in the Age of Data Protection: A Legal Comparative Study of GDPR, India's DPDP Act and Uzbekistan Law on Personal Data

Khushnazar Juraev¹ 

Lecturer at Department of Law and Technologies
Tashkent State University of Law
juraevkhushnazar@gmail.com

Submitted: 8-May, 2026

Accepted: 27-May, 2026

Published: 10-June, 2026

Vol. 3, No. 1, 2026. Sociometrics.us

Journal of Community, Law and
Diplomacy Sciences

***Corresponding author:**

Khushnazar Juraev
juraevkhushnazar@gmail.com

Copyright © 2026 by author(s) and
Scientific Research Publishing Inc. This
work is licensed under the Creative
Commons Attribution International
License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

This comparative study examines how three contemporary data-protection regimes the European Union's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection (DPDP) Act, and Uzbekistan's Law on Personal Data - address the concept and protection of digital identity. Through systematic analysis of statutory provisions, definitional frameworks, individual rights regimes, obligations imposed on controllers and processors, and enforcement mechanisms, this article evaluates whether and to what extent digital identity is legally recognized and substantively safeguarded. The analysis reveals that none of the three instruments explicitly denies the existence of digital identity; rather, each primarily frames protection around personal data as an informational or idem aspect of identity — stable identifiers and data points such as names, unique identifiers, and contact details. The study argues that this focus on the static, idem dimension leaves an important gap and a full protection of digital identity requires legal recognition and safeguarding of the "ipse" dimension the performative, contextual and reputational aspects of identity formed through online interactions, profiles, and algorithmic inferences. To address this gap, the researcher contends that data-protection laws should expand individual control mechanisms (including stronger rights over profiling, automated decision-making, reputation management and contextual consent), enhance transparency and redress concerning inference-based identity creation, and impose affirmative duties on data actors to prevent misuse of dynamic identity attributes. Strengthening these ipse-oriented protections will better enable individuals to manage their digital personhood and control how they are perceived and represented in the digital environment.

Key words: Digital identity; Data protection; GDPR; DPDP Act; Uzbekistan Law on Personal Data; Idem and Ipse; Profiling; Automated decision-making; Consent; Transparency; Reputation management; Individual data control; Algorithmic inferences

Introduction

In the contemporary digital ecosystem, digital identity encompasses the comprehensive online representation of individuals, businesses, and artificial entities, yet it remains without a universally accepted legal definition in international treaty law or national statutes. As explored in the paper, this legal vacuum is increasingly problematic in algorithmic environments where an individual's "digital person" is constructed via multi-layered platforms, biometric indices, and data tracking. Legal and sociological theories, including Helen Nissenbaum's contextual integrity and Paul Ricoeur's philosophy of personal identity, highlight a fundamental tension between the right to privacy and the right to digital identity. While privacy frameworks function primarily as informational data-management regimes, they structurally treat individuals as passive data subjects rather than narrative agents. Consequently, existing legislative models leave a profound structural gap: they safeguard the idem dimension (the static, verifiable data points like names, identifiers, and biometrics) while leaving the ipse dimension (the performative, contextual, and reputational selfhood shaped by algorithmic inferences and online interactions) fundamentally unguarded. This study addresses this critical gap by examining how current frameworks fail to empower individuals as narrative agents capable of contesting or redefining their digital personas in the face of pervasive corporate and state profiling.

Methodology

To evaluate these legal architectures, this study employs a qualitative, comparative legal research methodology that systematically analyzes three data protection regimes chosen for their geopolitical diversity and regulatory maturity: the European Union's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection (DPDP) Act, 2023, and the Republic of Uzbekistan's Law "On Personal Data" (LRU-547). The primary source materials examined in comprise black-letter statutory texts, legislative recitals, relevant international instruments like the United Nations Convention on Cybercrime, and foundational judicial precedents such as the Court of Justice of the European Union's *Google Spain* decision. These frameworks are evaluated through a standardized comparative matrix centered on four core variables: definitional scope, data subject rights regimes, obligations imposed on data fiduciaries or controllers, and sovereign enforcement mechanisms. Crucially, the analysis transcends conventional legal interpretation by applying Ricoeur's philosophical typology to map these statutory variables against the idem (sameness) and ipse (selfhood) dimensions of digital identity. This comparative approach enables the study to isolate systemic, normative gaps within rights-based, fiduciary-based, and state-centric regulatory models, ultimately establishing a robust framework for the future expansion of dynamic, individual-centric identity protections.

Result and Discussion

1. Digital Identity and the Fragmented Self

Digital identity refers to the totality of an individual's or entity's representation within the digital environment. It encompasses not only human beings but also the online representation of businesses, organizations, and artificial agents. Despite the pervasive role that digital identity plays in modern commerce, governance, and social life, there is as yet no universally accepted legal definition of the term. Roger Clarke, in a foundational contribution to this field, introduced the concept of the "digital persona" — a model of an individual's public personality based on data, constructed and deployed as a proxy for that individual in digital interactions¹. More recently, Marga Robles-Carrillo has elaborated on the multi-dimensional nature of digital identity, underscoring the continued absence of a settled legal definition in international instruments and proposing a functional taxonomy of its constituent components².

This conceptual vacuum persists even in the modern treaty law. The United Nations Convention on Cybercrime, concluded on 26 October 2025 in Hanoi, Vietnam, comes closest to addressing the concept through Article 2(g), which defines "personal data" as any information relating to an identified or identifiable natural person — an informational framing that captures the *idem* dimension of identity but leaves its performative and reputational dimensions unaddressed. Similarly, the Convention on Cybercrime adopted in Budapest in 2001 (the "Budapest Convention") does not define digital identity, although its provisions on computer-related forgery, fraud, and the misuse of devices implicitly acknowledge that identity attributes have value and that their unauthorized manipulation constitutes a cognizable harm warranting criminal sanction³.

Since there is no particular definition of digital identity in these international conventions, scholars have proposed their own formulations. Professor Claire Sullivan defines digital identity as "the sum of all digitally available information about an individual, regardless of its degree of validity, its form, or its accessibility⁴". This broad definition has the virtue of capturing the full informational surface area of digital identity — including inaccurate, incomplete, and inaccessible data — and of resisting any artificially narrow identification of digital identity with verified or official data alone. For example, a lawyer can have a professional user name on Instagram and a name which is not so serious for his gaming profiles, though both the identities belong to him. Digital identity can be analyzed through several core components: (a) *identifiers*, such as usernames, email addresses, and digital certificates; (b) *attributes*, such as date of birth, address, and employee identifiers; (c) *credentials*, such as passwords, biometric signatures, digital keys, and tokens; and (d) *activities*, such as search history and digital footprint⁵.

¹ Clarke, R. (1994). The digital persona and its application to data surveillance. *The Information Society*, 10(2), 77–92.

² Robles-Carrillo, M. (2024). Digital identity: An approach to its nature, concept, and functionalities. *International Journal of Law and Information Technology*, 32. <https://doi.org/10.1093/ijlit/eaee019>.

³ Council of Europe, *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, opened for signature 23 November 2001, Arts. 7–8 (computer-related forgery and fraud).

⁴ Robles-Carrillo, Marga. (2024). Digital identity: an approach to its nature, concept, and functionalities. *International Journal of Law and Information Technology*. 32. 10.1093/ijlit/eaee019.

⁵ Robles-Carrillo (2024), *supra* note 2.
<https://sociometrics.us/index.php/jclds>

These components are distributed across three conceptual layers. The *official layer* contains data that uniquely identifies a person by reference to government records — name, date of birth, national identification number, passport details, and electronic signatures. The *biometric layer* encompasses physiological and behavioral data, including facial recognition, fingerprints, iris patterns, voice, and genetic data. The *platform layer* comprises usernames, user-generated content, metadata, and search-engine indexing⁶. Collectively, these layers constitute what Daniel Solove has called the “digital person” — an information-based construct that can acquire legal and social significance independent of the natural person it represents⁷.

2. Dimensions of Digital Identity

2.1. Objective versus Subjective Identity

The philosophical distinction between objective and subjective identity offers a useful framework for analyzing digital identity. Akeel Bilgrami, in his foundational essay on the meaning of identity, explains that “subjective identity” refers to how an individual conceives of themselves, while “objective identity” refers to how that individual may be viewed independently of their self-conception⁸. Transposed to the digital context, objective identity consists of official documents, stable data points, and externally assigned identifiers — that which can be verified and attributed without reference to the individual's self-understanding — whereas subjective identity encompasses the values, beliefs, cultural affiliations, and self-presentations through which an individual chooses to define themselves online.

A person may objectively be a lawyer — possessing the requisite qualifications and professional license — while subjectively identifying primarily as a social activist or educator. Equally, an individual may be classified under a particular demographic or religious category in a database while subjectively rejecting that classification. These divergences become particularly acute in algorithmic environments, where profiling processes aggregate objective data to generate inferences about subjective identity attributes that the individual may never have disclosed or endorsed, and those inferences may then serve as the basis for consequential decisions.

2.2. Idem and Ipse Identify in the Social Web

The most theoretically productive distinction for analyzing digital identity is drawn from Paul Ricoeur’s philosophical account of personal identity in *Oneself as Another* (1992)⁹. Ricoeur argued that human identity is not reducible to the mere persistence of stable physical or biographical features. Identity also encompasses a second dimension — *ipse* (selfhood) —

⁶ Ibid.

⁷ Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York University Press, pp. 1–15.

⁸ Bilgrami, A. (2006). Notes toward a definition of “identity”. *Daedalus*, 135(4), 5–15.

⁹ Ricoeur, P. (1992). *Oneself as another* (K. Blamey, Trans.). University of Chicago Press. (Original work published 1990 as *Soi-même comme un autre*, Éditions du Seuil.)

<https://sociometrics.us/index.php/jclds>

which concerns the subject's capacity to remain faithful to its commitments and to narrate a coherent self even through transformation and change. Ricoeur's key insight is that a person is not only a set of stable traits but also a living, acting self who evolves while remaining recognizably *itself*.

2.2.1. Idem Identity

Idem identity denotes sameness or continuity over time. It answers the question: *what remains the same about this person across time?* Idem identity is constituted by stable, recognizable features — name, physical characteristics, biographical facts, habitual traits — that enable the identification of the same individual across different contexts and moments. A person who was reticent in school but later became a confident lawyer retains the recognizable physical and biographical markers that constitute their idem identity; the person is identifiable as the same individual despite their personal development.

2.2.2. Ipse Identity

Ipse identity, by contrast, denotes selfhood — the subject's first-person self-understanding and capacity for self-commitment. It answers the question: *who is this person as an acting, narrating self?* Ipse identity accommodates change while preserving the coherent subjectivity of the individual; it is constituted through promise-keeping, moral agency, and narrative self-understanding. A person may successively identify as an engineer, a lawyer, and a teacher, yet maintain a consistent commitment to justice and public service; ipse identity captures this inner continuity of selfhood through occupational and circumstantial transformation.

2.3. Idem and Ipse Identity in the Digital Space

2.3.1. Idem in Digital Identity

In the digital context, *idem* identity corresponds to the verifiable, stable data used to confirm that a person is who they claim to be — name, date of birth, identification number, biometric credentials, login data, and platform registration information. Whenever a banking application authenticates a user against a stored customer identifier or one-time password, it is performing an idem verification: the system confirms that the presented data matches the registered data, affirming sameness across time.

2.3.2. Ipse in Digital Identity

Ipse identity in the digital space refers to the individual's reflective selfhood, narrative autonomy, and ongoing self-presentation online. It is expressed through social media profiles, curated content, privacy choices, value-laden statements, and the deliberate management of online presence. Ipse identity evolves, can be re-narrated, and resists reduction to a fixed set of data points. Crucially, it is also the dimension of identity most vulnerable to distortion by algorithmic inference: a platform's profile of a user may diverge

radically from that user's self-understanding, yet the inferred profile may acquire legal and commercial consequences as weighty as those of verified idem data — without any mechanism for the individual to contest or correct it.

3. The Right to Digital Identity

The advent of information technology has furnished individuals with the tools to construct, modify, and project a digital image within the digital environment. Platforms provide the technical and contractual infrastructure through which digital identities are created and — to varying degrees — controlled by their subjects. This conferral of identity-shaping capacity generates a corresponding normative expectation: individuals who invest in constructing a digital identity have a legitimate interest in defending its integrity and accuracy against unauthorized interference.

This expectation has deep roots in legal theory. Samuel Warren and Louis Brandeis, in their seminal 1890 article, argued that the development of modern law required recognition of an individual's "right to be let alone" — a right of inviolate personality extending to the protection of personal information and reputational standing¹⁰. Alan Westin subsequently defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others¹¹. Helen Nissenbaum further extended this analysis through her theory of contextual integrity, arguing that privacy protection is not simply about secrecy but about the appropriate flow of information: information flows appropriately when it conforms to the norms of the context in which it originated¹². A digital profile constructed by algorithmic inference and deployed across contexts violates this principle even where no data breach has occurred.

S.I. Benn reinforces this from the perspective of personal autonomy: if law takes seriously the freedom of individuals to define themselves and their place in society, it must provide legal tools that enable each person to be whoever they choose to be in the contexts of their choosing¹³. This article endorses that view, arguing that individuals seek not merely the protection of data already held by digital platforms but also the capacity to shape, contest, and redefine their digital persona over time. Daniel Solove's analysis supports this framing: existing data protection frameworks treat the individual as an informational subject rather than as a narrative agent with a stake in how their digital persona is constituted and projected, producing a structural asymmetry in which the idem dimension of identity receives formal protection while the ipse dimension remains largely unguarded¹⁴.

¹⁰ Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.

¹¹ Westin, A. F. (1967). *Privacy and freedom*. Atheneum, p. 7.

¹² Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, pp. 127–157.

¹³ Benn, S. I. (1984). Privacy, freedom, and respect for persons. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 223–244). Cambridge University Press.

¹⁴ Solove (2004), *supra* note 7, at 1–15.
<https://sociometrics.us/index.php/jclds>

This structural gap is the central concern of the present article. Current data protection frameworks are, in essence, data management regimes: they regulate who may process personal data, under what conditions, and subject to what procedural safeguards. They do not recognize the individual as a narrative agent entitled to determine how their digital persona is constituted, nor do they impose duties on data actors to respect the coherence and accuracy of inferred identity profiles.

4. Right to Privacy versus Right to Digital Identity

Data protection laws across the world are primarily oriented toward the protection of static, informational attributes — the *idem* dimension of personal identity. By governing who may process an individual's data and under what conditions, these laws deliver a degree of informational privacy. This article, however, maintains a fundamental conceptual distinction between the right to privacy and the right to digital identity.

The right to privacy in the digital context relates to the protection of personal data already generated or held by controllers: it is fundamentally a right of non-interference with one's informational sphere. The right to digital identity is broader: it encompasses the right to create, modify, contest, and protect one's digital persona — the totality of the representations through which an individual is perceived and engaged within the digital environment. As Nissenbaum's theory of contextual integrity illustrates, the harm from inappropriate data flows is not purely informational but also reputational and relational — it affects how individuals are understood, classified, and treated by others¹⁵.

This distinction carries significant practical implications. The right to privacy is subject to well-recognized limitations on grounds of national security, public order, and public interest. If the right to digital identity is conceptually collapsed into the right to privacy, it becomes vulnerable to the same restrictions; a state may invoke national security to override both simultaneously. Recognizing a discrete right to digital identity — grounded in principles of autonomy, dignity, and narrative self-determination — would require an independent analysis of necessity and proportionality before any limitation could be justified, affording structurally stronger protection against both private actors and state intrusion.

Viktor Mayer-Schönberger's analysis of the societal consequences of perpetual digital memory underscores the urgency of this distinction: in an environment where past digital traces are never erased and can be indefinitely aggregated, the ability to construct and modify one's digital narrative becomes a fundamental condition of individual autonomy¹⁶. The right to be forgotten — examined in greater detail below — represents a partial recognition of this principle, but, as will be argued, it falls short of constituting a comprehensive right to digital identity.

¹⁵ Nissenbaum (2010), *supra* note 12.

¹⁶ Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.
<https://sociometrics.us/index.php/jclds>

5. GDPR and the European Courts view on Digital Identity

The European Union's General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") is widely regarded as the most comprehensive and influential data protection instrument currently in force, establishing the global benchmark for data subject rights, controller obligations, and enforcement mechanisms¹⁷. Yet, despite its comprehensiveness, the GDPR contains no definition of "digital identity" — a gap all the more striking given that identity protection is a core rationale for the Regulation. Recital 1 of the GDPR explicitly states that the protection of natural persons with regard to the processing of personal data is a fundamental right, while Recital 4 acknowledges that this right is not absolute and must be considered in relation to its function in society, balanced against other fundamental rights in accordance with the principle of proportionality.

Chapter III of the GDPR (Articles 12–23) establishes a catalogue of data subject rights, several of which bear directly on digital identity. Article 16 (right to rectification) enables individuals to correct inaccurate personal data, providing a partial mechanism for idem identity management. Article 17 (right to erasure, commonly termed the "right to be forgotten") allows individuals to require deletion of personal data in defined circumstances. Article 21 (right to object) and Article 22 (rights in relation to automated decision-making and profiling) extend some protection to the ipse dimension, permitting individuals to resist automated profiling and to request human review of consequential automated decisions.

The right to be forgotten was judicially recognized by the Court of Justice of the European Union even before the GDPR's adoption. In *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12, 2014), the Court held that individuals may require search engine operators to delist links to web pages containing personal information that is outdated, inadequate, or no longer relevant to the original purpose of processing¹⁸. This decision marked a paradigmatic shift: for the first time, an individual was afforded a legal instrument to control not merely the disclosure of their data but the accessibility of information about their past — an instrument of ipse identity management that allows a person to shape how they are perceived in the present by modifying the digital record of the past.

Jeffrey Rosen has characterized this development as the emergence of a fundamental right against the tyranny of perpetual digital memory — a right that enables individuals to escape their documented past and to construct a coherent self-narrative in the present¹⁹. Viktor Mayer-Schönberger similarly situates the right to be forgotten within a broader argument for restoring the natural human capacity for forgetting: an environment in which nothing is forgotten impairs both individual development and social renewal, making structured

¹⁷ Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer, pp. 1–5.

¹⁸ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317 (Court of Justice of the European Union, 13 May 2014).

¹⁹ Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, 64, 88–92.
<https://sociometrics.us/index.php/jclds>

mechanisms for deletion a normative necessity rather than a technical luxury²⁰.

Yet the limitations of Article 17 must be candidly acknowledged. The right to erasure is subject to significant exceptions: it does not apply where processing is necessary for the exercise of freedom of expression or information, for compliance with a legal obligation, for archiving, scientific, historical, or statistical purposes in the public interest, or for the establishment, exercise, or defense of legal claims. These exceptions reflect a necessary legislative balancing of competing rights, but their breadth means that the right to be forgotten cannot function as an unconditional guarantee of digital identity control.

Beyond Article 17, the GDPR's consent provisions (Article 7), transparency obligations (Articles 12–14), data minimization principle (Article 5(1)(c)), and purpose limitation principle (Article 5(1)(b)) collectively impose structural constraints on the construction of inferred digital profiles. Nadezhda Purtova has argued, however, that the broad interpretation of “personal data” — extended through Recitals 26 and 30 to online identifiers, location data, IP addresses, and cookie identifiers — risks rendering the Regulation simultaneously overinclusive and underenforced: when every data point constitutes personal data, the concept loses its discriminating normative power, and enforcement resources are spread too thin to be effective²¹. The practical implication for digital identity protection is that GDPR norms may reach broadly across the idem dimensions of identity while remaining inadequately calibrated to the ipse dimensions, where the stakes of inaccurate or manipulative profiling are highest.

In sum, the GDPR constitutes a significant — but incomplete — contribution to digital identity protection. Its rights framework provides meaningful tools for managing idem identity, and its provisions on profiling and automated decision-making extend some protection to ipse identity. Nevertheless, the Regulation does not directly address the construction, contestation, and modification of digital personas as such. A further normative development is required to close this gap.

6. Law of Republic of Uzbekistan on Personal Data LRU-547

Uzbekistan's principal legislative instrument in this domain is the Law of the Republic of Uzbekistan “On Personal Data”, enacted on 2 July 2019 (Law No. LRU-547). Article 4 of the Law defines personal data as “information recorded on electronic, paper and (or) other tangible media that relates to a specific individual or makes it possible to identify him/her”. This definition, like those in the GDPR and the DPDP Act, frames data protection in informational terms, without reference to the relational, performative, or reputational dimensions of digital identity. The Law neither defines “digital identity” nor contains provisions specifically addressing the construction or modification of digital personas.

²⁰ Mayer-Schönberger (2009), *supra* note 16.

²¹ Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40–81.
<https://sociometrics.us/index.php/jclds>

A careful analysis of the Law's protective priorities reveals a strong orientation toward the *idem* dimension of personal identity. Most instructively, Article 27(1) imposes a mandatory data localization requirement for biometric and genetic data: such data must be stored on servers physically located within the territory of Uzbekistan, and this requirement cannot be derogated from by the data subject's consent. Other categories of personal data may, by contrast, be transferred outside the territory of Uzbekistan with consent. This asymmetric localization regime reflects a legislative judgment that biometric and genetic data — the most irreplaceable and immutable components of *idem* identity — warrant the strongest territorial protection, while more dynamic data may be permitted to circulate more freely.

While the data localization provision represents a meaningful safeguard for core *idem* identity attributes, the Law does not provide equivalent protection for the *ipse* dimension. It contains no provisions addressing profiling, automated decision-making, or reputation management comparable to those in Chapter III of the GDPR. Individual control mechanisms are correspondingly limited: the consent framework provides the foundational legal basis for processing, but the Law does not establish differentiated rights to contest inferred profiles or to demand transparency regarding inference-based identity constructs. Article 27's guarantee — that the state ensures the protection of personal data stored within its territory — reflects a state-centric rather than individual-centric model of protection: one that secures sovereign control over identity infrastructure but does not fully empower individuals to manage their own digital personas.

This state-centric approach contrasts with the GDPR's rights-based architecture and the DPDP Act's fiduciary model, and may be explained partly by the specific administrative and regulatory context of Uzbekistan, as well as by the relative novelty of comprehensive data protection legislation in Central Asia. As data governance frameworks in Uzbekistan continue to mature under the Digital Uzbekistan 2030 strategy, future legislative revision may present an opportunity to introduce *ipse*-oriented protections aligned with the evolving international consensus.

7. Digital Personal Data Protection Act, 2023 in India

India's Digital Personal Data Protection Act, 2023 ("DPDP Act") is the most recently enacted of the three instruments under examination. Enacted in August 2023, it constitutes India's first comprehensive personal data protection statute, replacing earlier piecemeal frameworks that had developed under the Information Technology Act, 2000. As the most recent of the three instruments, the DPDP Act had the benefit of extended comparative experience with the GDPR and a generation of national data protection laws worldwide; this context makes its omissions all the more significant.

The DPDP Act does not define "digital identity". Section 2(h) defines "data" broadly as "a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means". Section 2(t) defines "personal data" as "any data about an individual who is identifiable by or <https://sociometrics.us/index.php/jclds>

in relation to such data." Notwithstanding the apparent breadth of the phrase "any data", the operative framework of the Act centers on the idem dimension: it is principally concerned with the fair processing of identifying data, the appointment of a "Consent Manager", liability for unauthorized processing or breach, and the administrative machinery of enforcement.

The DPDP Act introduces the concept of the "Data Fiduciary" — an entity that determines the purpose and means of processing personal data — and imposes obligations of notice, consent, accuracy, and breach notification on Data Fiduciaries vis-à-vis "Data Principals" (the individuals to whom personal data relates). This fiduciary framing introduces a relational and trust-based dimension absent from the GDPR's more contractualist model, creating potential for a richer account of individual control. A Data Fiduciary, in principle, owes duties to its Data Principal analogous to those owed by a trustee to a beneficiary. However, the Act does not translate the fiduciary relationship into specific rights over profiling, automated decision-making, or digital persona management; the ipse dimension of digital identity therefore remains largely unaddressed.

Conclusion

The comparative analysis of the GDPR, India's DPDP Act, and Uzbekistan's Law on Personal Data reveals a common structural limitation: all three instruments protect personal data primarily as a vehicle for safeguarding the static, idem dimension of digital identity — stable identifiers, biographical facts, and biometric data. None of the three explicitly denies the significance of digital identity as a broader legal concept, but none provides a framework adequate to the protection of its ipse dimension: the performative, narrative, and reputational aspects of the self as constituted and contested in the digital environment.

This structural gap has concrete practical implications. In the absence of robust ipse protections, individuals remain vulnerable to having their digital personas constructed, inferred, and projected by algorithmic systems without adequate mechanisms for contestation, correction, or accountability. The consequences — misclassification, reputational harm, discriminatory profiling, and loss of narrative self-determination — are not adequately addressed by existing informational privacy frameworks, which were designed to manage data flows rather than to protect the coherence of digital personhood.

To close this gap, data protection law must evolve in at least three directions. First, individual control mechanisms should be expanded: rights over profiling, automated decision-making, and reputation management should be strengthened, and consent frameworks should be redesigned to accommodate the contextual sensitivity of identity-forming data flows, in line with the theory of contextual integrity²². Second, transparency obligations concerning inference-based identity construction should be enhanced, ensuring that individuals can understand and meaningfully challenge the digital profiles constructed about them by

²² Nissenbaum (2010), *supra* note 12.
<https://sociometrics.us/index.php/jclds>

algorithmic systems. Third, affirmative duties should be imposed on data actors — both controllers and platforms — to prevent misuse of dynamic identity attributes and to ensure that inferred profiles do not acquire legal or commercial consequences that the individual has not endorsed.

REFERENCES

- [1] A. Bilgrami, “Notes toward a definition of ‘identity’”, *Daedalus*, vol. 135, no. 4, pp. 5–15, 2006.
- [2] S. I. Benn, “Privacy, freedom, and respect for persons”, in *Philosophical Dimensions of Privacy: An Anthology*, F. D. Schoeman, Ed. Cambridge, UK: Cambridge University Press, 1984, pp. 223–244.
- [3] R. Clarke, “The digital persona and its application to data surveillance”, *The Information Society*, vol. 10, no. 2, pp. 77–92, 1994.
- [4] Council of Europe, “Convention on Cybercrime (Budapest Convention)”, ETS No. 185, Nov. 23, 2001. [Online]. Available: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- [5] European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, *Official Journal of the European Union*, L 119, pp. 1–88, May 4, 2016.
- [6] L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford, UK: Oxford University Press, 2014.
- [7] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317, Court of Justice of the European Union, May 13, 2014.
- [8] Parliament of India, *Digital Personal Data Protection Act*, No. 22 of 2023, Aug. 11, 2023.
- [9] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ, USA: Princeton University Press, 2009.
- [10] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, USA: Stanford University Press, 2010.
- [11] N. Purtova, “The law of everything: Broad concept of personal data and future of EU data protection law”, *Law, Innovation and Technology*, vol. 10, no. 1, pp. 40–81, 2018.
- [12] P. Ricoeur, *Oneself as Another*, K. Blamey, Trans. Chicago, IL, USA: University of Chicago Press, 1992.
- [13] M. Robles-Carrillo, “Digital identity: An approach to its nature, concept, and functionalities”, *International Journal of Law and Information Technology*, vol. 32, 2024, doi: 10.1093/ijlit/eaee019.

- [14] J. Rosen, "The right to be forgotten", *Stanford Law Review Online*, vol. 64, pp. 88–92, 2012.
- [15] D. J. Solove, *The Digital Person: Technology and Privacy in the Information Age*. New York, NY, USA: New York University Press, 2004.
- [16] C. Sullivan, *Digital Identity: An Emergent Legal Concept*. Adelaide, SA, Australia: University of Adelaide Press, 2011.
- [17] United Nations, "United Nations Convention on Cybercrime", adopted Oct. 26, 2025, Hanoi, Vietnam.
- [18] Republic of Uzbekistan, *Law of the Republic of Uzbekistan "On Personal Data"*, No. LRU-547, Jul. 2, 2019.
- [19] P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer, 2017.
- [20] S. D. Warren and L. D. Brandeis, "The right to privacy", *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, Dec. 1890.
- [21] A. F. Westin, *Privacy and Freedom*. New York, NY, USA: Atheneum, 1967.