The Digital Persona in the Algorithmic Age: Legal Frameworks, Data Commercialization, and the Protection of Identity

Mahdi Mohammadzadeh

Abstract

The transformation of identity in the digital age has become one of the defining legal and philosophical issues of contemporary society. As personal data increasingly functions as a source of economic value, a means of social classification, and a tool of algorithmic governance, the law has been forced to reconsider the meaning of personhood, privacy, and autonomy. This essay examines the evolution of digital identity between 2024 and 2026 through a legal and socio-technical lens. It argues that digital identity can no longer be treated as a secondary reflection of the physical person, but must instead be understood as a dynamic and vulnerable extension of the self. The discussion begins with the conceptual transformation of identity from a static, identificatory model to a dynamic, identitary profile. It then addresses the commercialization of personal data, especially within the framework of data as counter-performance and the legal limits of contractual freedom. The essay next considers algorithmic profiling, the rise of large language models, and the collision between the GDPR and the EU AI Act. It then turns to generative identity theft and the growing legal response to deepfakes, before concluding with the unresolved issue of post-mortem privacy and digital inheritance. The central claim is that the protection of human dignity in the algorithmic age requires a legal order in which data processing remains subordinate to the free development of personality, rather than to the imperatives of extraction, prediction, and monetization.

1. Introduction

The rise of digital technologies has fundamentally altered the way identity is created, represented, and regulated. In earlier legal traditions, identity was largely understood in relation to the physical body and the official attributes by which a person could be recognized in civil life: name, birth date, image, and legal status. In contemporary digital society, however, identity is no longer limited to these stable markers. It is increasingly

produced through a constellation of data traces, behavioral patterns, algorithmic inferences, platform interactions, and machine-generated representations [1, 7, 2].

This transformation has profound consequences. Personal data is no longer merely descriptive. It is now productive. It shapes advertising, access to services, employment decisions, insurance pricing, platform visibility, and political targeting. A person's digital profile is not simply a record of past actions. It is also a mechanism through which future opportunities and constraints are determined. In this sense, digital identity has become both economic infrastructure and social power [1, 12, 4].

Legal systems have responded unevenly to this development. The European Union has attempted to build a comprehensive architecture through instruments such as the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act, and the AI Act [3, 22]. These measures seek to regulate different aspects of the data economy, platform governance, and algorithmic systems. Yet the pace of technological change has placed increasing pressure on these frameworks. Profiling practices have become more granular and opaque. Generative AI systems are trained on vast quantities of scraped data. Deepfakes now enable the synthetic reproduction of a person's face, voice, and mannerisms. At the same time, the law remains underdeveloped in areas such as digital inheritance and post-mortem privacy [6, 28].

This essay argues that the digital age requires a reconceptualization of legal identity around three principles. First, identity must be understood as dynamic, relational, and informational rather than merely static and administrative. Second, personal data must not be reduced to a simple commodity governed by market exchange. Third, legal protections must extend across the full temporal arc of the person, including the afterlife of digital remains. The defense of human dignity in the algorithmic age depends on maintaining these principles against the economic logic of surveillance and extraction [1].

2. From Static Identification to the Dynamic Digital Self

One of the most important legal developments in the modern understanding of identity has been the shift from a static to a dynamic conception of the person. The older, static model of identity was centered on identification. Its main function was to distinguish one individual from another for purposes of administration, public order, and civil status. This model treated identity as a set of objective and relatively unchanging attributes. The legal system's role was to protect these attributes against impersonation, falsification, or misuse.

In digital society, this static model is no longer sufficient. Identity is increasingly shaped by the circulation of information in networked environments. Individuals are represented

not only through official documents and legal registries, but also through search results, social media activity, biometric markers, consumer histories, geolocation patterns, and predictive scores. These fragments combine into what may be called a dynamic identitary profile [7, 11].

The legal significance of this shift lies in the recognition that a person has an interest not merely in being correctly named or visually represented, but in being represented truthfully in the broader sense of their social, intellectual, and personal reality. A distorted digital profile can alter how others perceive the person, how institutions classify them, and how systems allocate rights and opportunities. In that respect, digital identity implicates not only privacy but also personality, dignity, and self-development [**?**, 1].

This more dynamic understanding of identity is especially visible in constitutional traditions that place the person at the center of legal order. Under such traditions, the law is not limited to protecting economic interests or administrative certainty. It must also safeguard the conditions under which the person can develop freely in society. In the Italian context, the constitutional grounding of personal identity is closely linked to Articles 2 and 3 of the Constitution, which protect inviolable rights and require the legal order to secure the full development of the individual [**?**]. Digital identity therefore becomes a constitutional concern. If online representations are manipulated, fragmented, or rendered inaccurate through algorithmic processes, the harm is not merely reputational. It strikes at the individual's ability to exist in public life as the author of their own social meaning.

The emergence of digital identity systems has further complicated this transformation. State-backed systems such as electronic identification frameworks, digital wallets, and interoperable authentication services are designed to provide reliable access to public and private services [8, 9]. These systems primarily address the identificatory side of digital identity. Yet the broader digital ecosystem is dominated not by the state but by private platforms, data brokers, advertising networks, and AI developers. These actors do not merely verify identity. They produce and monetize it.

This division generates serious dilemmas. The first is contextual. A person can inhabit multiple online identities at once, including pseudonymous, professional, intimate, and experimental selves. The second is conceptual. There is no universal agreement about whether digital identity should be defined as a verified legal correspondence, a bundle of claims, or a shifting pattern of behavior. The third is functional. Digital identity systems can support inclusion and efficiency, but they can also intensify surveillance and dependency [2, 10]. These dilemmas show that the digital self cannot be regulated through technical design alone. It requires a normative framework grounded in rights, accountability, and structural limits on power [1].

3. The Commodification of Personal Data

The expansion of digital identity is inseparable from the commodification of personal data. In the contemporary platform economy, human behavior is continuously translated into information that can be captured, analyzed, and sold. Browsing patterns, location history, attention metrics, emotional responses, and social relationships have all become inputs for commercial systems. The individual thus appears in the market not only as a consumer but also as a source of raw material [4, 12].

This development has led to a long-running legal debate over the status of personal data. One view treats data as a form of property that can be owned, transferred, and exchanged. Another rejects this approach and insists that personal data is bound up with personality and dignity in a way that makes it fundamentally resistant to ordinary commodification. A more convincing approach distinguishes between personal data as such and the economic uses derived from processing it [14, 15].

Data does not behave like an ordinary commodity. Its value does not lie merely in possession, but in aggregation, analysis, inference, and recombination. What is monetized is not simply the data point itself, but the capacity to transform that data into predictive knowledge, advertising precision, risk scoring, and behavioral influence. This is why contract law alone cannot provide an adequate regulatory framework. A contract may authorize the exchange of access, content, or services, but it cannot override the mandatory principles that govern data processing.

The doctrine of data as counter-performance illustrates this tension vividly. Under modern digital consumer law, services may be supplied not only in exchange for money but also in exchange for personal data [13, 16]. This reflects the practical reality that many so-called free services are financed through surveillance and targeted advertising. Yet once data is treated as a form of payment, a problem emerges. The logic of exchange suggests reciprocity and performance. The logic of data protection insists on ongoing rights: transparency, minimization, purpose limitation, withdrawal of consent, and erasure.

The result is a structural conflict between the bilateral logic of contract and the rights-based logic of data protection. That conflict becomes clearest where consent is withdrawn. In ordinary contract doctrine, withdrawal may count as non-performance. Under data protection law, however, consent must remain revocable and genuinely free. For that reason, the commercialization of personal data must always remain subordinate to the legal protection of informational self-determination [17, 15].

4. Pay-or-Consent and the Limits of Contractual Freedom

The legal limits of data commercialization became especially visible in the controversy surrounding pay-or-consent models. Under these models, a platform offers users a binary choice: either accept extensive tracking and personalized advertising, or pay a subscription fee to access a version of the service with reduced data processing. At first glance, this may appear to preserve user choice. In reality, it raises serious questions about coercion, inequality, and the meaning of freely given consent [18, 20].

Consent under data protection law is valid only when it is informed, specific, and freely given. This requirement is not satisfied merely because the user clicks a box or selects one of two presented options. The surrounding conditions matter. Where a dominant platform conditions meaningful participation in social or economic life on surrendering data, the resulting choice may be formal rather than substantive. A fee-based alternative does not necessarily cure the problem, especially if the fee is high enough to make privacy effectively unaffordable [18, 19].

This issue reveals the inadequacy of understanding privacy through the lens of consumer preference alone. Privacy is not a luxury feature. It is tied to autonomy, equality, and protection against exploitation. If the law permits platforms to charge for the non-extractive version of their services while making surveillance the default condition of access, then informational self-determination becomes stratified by wealth.

That outcome is difficult to reconcile with the constitutional foundations of data protection. The right to privacy is not designed simply to correct market failures. It protects a sphere of freedom within which the person can think, communicate, associate, and develop without constant monitoring. For that reason, contract cannot be permitted to serve as the mechanism by which individuals are pressured to waive rights that the legal order treats as fundamental.

The pay-or-consent model also highlights the imbalance of power between platforms and users. Large platforms often operate as gatekeepers. They structure social interaction, advertising markets, and public attention at scale. Their bargaining power is not comparable to that of individual users. This imbalance undermines the assumption that platform terms are the product of meaningful negotiation. In practice, they are unilaterally imposed governance regimes [19, 21].

The broader lesson is that freedom of contract has limits when the subject matter of the agreement concerns the conditions of personhood in digital society. Data protection law sets mandatory floors below which no contract should fall. A platform may innovate in service design, but it cannot purchase unrestricted authority over the digital self.

5. Algorithmic Profiling and the Expansion of Informational Power

Algorithmic profiling stands at the center of the modern data economy. It is the process through which personal data is analyzed to evaluate, classify, and predict aspects of a person's behavior, preferences, reliability, health, interests, or future actions. Profiling gives digital identity its operational force. Without it, most contemporary advertising, recommendation systems, dynamic pricing models, and automated decision systems would not function as they do [3, 12].

The power of profiling lies in its ability to transform scattered traces into actionable judgments. A set of isolated behaviors may appear insignificant when viewed separately. Once aggregated and processed, those same traces can reveal intimate patterns. They can suggest political affiliation, emotional vulnerability, likely purchasing habits, creditworthiness, or susceptibility to persuasion. Profiling therefore turns data into social and economic leverage.

Data protection law recognizes the risks and attempts to regulate them through layered safeguards. These include principles of fairness and transparency, restrictions on purpose expansion, rights to object, and heightened protections against solely automated decisions that produce legal or similarly significant effects [3, 23]. Yet the practical enforcement of these safeguards remains difficult. Profiling systems are often opaque by design. Their inferences are probabilistic, proprietary, and continuously updated.

The challenge is not only individual but structural. Profiling reshapes the relationship between the person and institutions. Decisions are increasingly based not on what a person has done, but on what systems infer that they are likely to do. This shift from retrospective judgment to predictive classification alters the normative basis of governance. It encourages intervention before action, risk sorting before wrongdoing, and optimization before deliberation.

For these reasons, profiling should not be treated merely as a technical method of sorting information. It is a mode of power that intervenes in the formation of identity itself. By continuously assigning meaning to conduct and predicting future behavior, profiling does not simply observe the self. It participates in its construction. That is why any serious legal response must go beyond disclosure and include stronger forms of accountability, contestability, and institutional oversight.

6. Large Language Models and the Crisis of Data Protection

The emergence of large language models has intensified existing tensions within data protection law. These systems are trained on enormous datasets collected from books,

websites, forums, repositories, and other publicly accessible sources. In practice, this often involves indiscriminate scraping of online content at a scale that far exceeds traditional forms of data collection [6, 23].

This creates a deep conflict with core data protection principles. Lawfulness becomes uncertain when the legal basis for mass scraping is unclear or contested. Purpose limitation is strained because data originally posted for communication, self-expression, employment, or community participation is later repurposed for training commercial AI systems. Data minimization is challenged by the very premise of model development, which rewards scale and breadth. Accuracy becomes problematic when models generate plausible but false statements about identifiable individuals [6, 12].

The issue is particularly acute with sensitive data. Public availability does not eliminate vulnerability. A person may disclose information in one context without consenting to its extraction into a general-purpose predictive system. The fact that information can be accessed on the open web does not mean it has been released into a legal void. Context, expectation, and proportionality remain relevant.

The EU AI Act seeks to address some of these concerns by introducing a risk-based governance framework for AI systems. It imposes obligations relating to transparency, documentation, human oversight, and fundamental rights impact assessment, especially for high-risk uses [22, 24]. Yet the AI Act does not replace data protection law. Product safety logic and fundamental rights logic perform different functions. A model may satisfy technical compliance requirements and still violate principles of fairness, necessity, or lawful processing.

What the rise of large language models makes plain is that the law can no longer treat mass data extraction as a neutral background condition of innovation. Model training is not merely a technical process. It is a social and legal act that redistributes informational power on a massive scale. If left inadequately regulated, it risks normalizing the idea that whatever can be scraped can be transformed into proprietary intelligence.

7. Generative Identity Theft and the Deepfake Problem

If profiling and language models challenge the boundaries of privacy law, deepfakes challenge the integrity of identity itself. Advances in generative AI now make it possible to create highly realistic synthetic images, videos, and audio recordings depicting people saying or doing things that never occurred. These technologies can imitate facial expression, tone of voice, cadence, and gesture with increasing precision [5, 27].

The harms caused by deepfakes are varied. On the individual level, they can be used for harassment, extortion, reputational sabotage, and non-consensual intimate imagery. On

the economic level, they facilitate fraud by simulating executives, relatives, or authority figures in real time. On the political level, they can be deployed to manipulate elections, spread disinformation, or undermine confidence in authentic media [5, 25, 26].

What makes generative identity theft especially serious is that it exploits the most recognizable aspects of the person: face, voice, mannerism, and social presence. It takes the external signs through which identity is ordinarily expressed and turns them into manipulable assets. In doing so, it collapses the distinction between representation and fabrication.

Traditional legal doctrines offer only partial remedies. The right of publicity may address unauthorized commercial exploitation of likeness, but it is fragmented and often limited in scope. Defamation law requires proof of false statements and reputational harm, which may not capture all forms of synthetic abuse. Privacy law may help in cases involving intimate content, but not in every instance of mimicry or deception. These gaps explain the growing push for targeted legislation [5, 34].

Recent initiatives have sought to criminalize certain categories of synthetic media, especially non-consensual sexual deepfakes and deceptive election-related content, while also imposing duties on platforms to remove harmful material quickly. At the same time, transparency obligations such as labeling and watermarking requirements aim to preserve some baseline distinction between human-created and machine-generated content [24, 22].

Yet regulation in this area must be carefully calibrated. Deepfake law cannot ignore free expression concerns. Satire, parody, artistic experimentation, and journalistic simulation may all involve synthetic media in ways that should not be prohibited outright. The challenge is to draw lines based on harm, deception, context, and consent. The deeper issue is epistemic as much as legal. Deepfakes contribute to a crisis of authenticity in which fabricated media undermines trust in genuine evidence itself [27].

8. Post-Mortem Privacy and Digital Inheritance

One of the least resolved questions in digital law concerns what happens to personal data after death. In physical life, inheritance law provides established rules for the transmission of property and the administration of estates. Digital life disrupts this framework. A deceased person may leave behind social media accounts, emails, cloud archives, cryptocurrencies, subscription histories, photographs, message threads, and AI-trainable personal records [28, 29].

The problem begins with classification. Some digital assets have clear economic value, such as cryptocurrency wallets or monetized accounts. Others are sentimental, such

as photo libraries or personal correspondence. Still others consist of access credentials, metadata, or relational communications involving third parties. Each category raises different questions about ownership, confidentiality, and control.

The issue is compounded by the relative absence of harmonized post-mortem privacy rules. Where privacy law does not protect the deceased directly, the governance of digital remains is often left to platform policies and contractual terms. This gives private companies significant authority over memory, access, deletion, and memorialization [30, 32].

This situation produces a paradox. Many individuals care deeply about their posthumous privacy and legacy, yet few take the steps necessary to manage those interests during life. As a result, families and executors face uncertainty, conflict, and emotional strain [30, 31]. Some are denied access to materials of sentimental value. Others gain access to intensely private communications that the deceased may never have wanted them to see.

A more coherent framework would begin by recognizing that autonomy does not end simply because biological life does. The digital traces of a person continue to shape reputation, memory, and relationships after death. They may also affect the privacy of living third parties. Post-mortem privacy should therefore be treated not as an anomaly but as an extension of the law's concern with dignity and personal integrity [28, 33].

Such an approach would support mechanisms for digital stewardship. Individuals should be able to specify in legally recognized form how different classes of digital assets are to be managed, preserved, transferred, or deleted. Executors should have clearly defined fiduciary powers, limited by privacy-sensitive duties. Platforms should not be free to determine the fate of digital remains solely through unilateral policy.

9. Conclusion

The digital age has transformed identity into a site of continuous production, contestation, and commercial exploitation. No longer reducible to official markers of civil status, identity now emerges through informational processes that classify, predict, reproduce, and monetize the person across multiple domains of life. The law cannot meet this challenge by relying on inherited distinctions alone. It must confront the reality that digital identity is dynamic, economically valuable, technically vulnerable, and constitutionally significant.

This essay has traced that reality across several interconnected developments. First, it showed how identity has moved from a static model of identification toward a dynamic model of representation and personality. Second, it examined the commodification of personal data and explained why contract law cannot be allowed to override the mandatory protections of data protection law. Third, it explored how profiling systems and large

language models intensify the asymmetry between individual persons and institutions capable of extracting and operationalizing behavioral data at scale. Fourth, it analyzed deepfakes as a form of generative identity theft that threatens both personal dignity and public trust. Finally, it argued that post-mortem privacy and digital inheritance expose a major gap in contemporary legal order.

The unifying lesson is clear. Personal data must not be treated merely as fuel for optimization. It is bound up with the development of personality, the exercise of freedom, and the conditions of democratic life. Legal frameworks such as the GDPR and the AI Act remain essential, but they must be interpreted and enforced in a way that resists the reduction of human beings to extractive profiles. Rights must be made operational against concentrated digital power, not just proclaimed in abstract form.

To protect human dignity in the algorithmic age, the legal system must preserve a basic normative priority: technology and markets should serve the person, not reconstruct the person as an instrument of technological and market logic. That principle is the foundation on which any just regime of digital identity must rest.

References

[1] Ruggiero, Domenico Giovanni, *Law, Ethics and Privacy in Information Management*, course materials, University of Campania Luigi Vanvitelli.

[2] *Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity*, *PMC*.

[3] Future of Privacy Forum, *GDPR and the AI Act Interplay: Lessons from FPF's ADM Case-Law Report*.

[4] *The Influence of Personal Data on Everyday Life: Theories, Case Studies, and Ethical Implications of Data Monetization and Privacy Challenges*.

[5] *Generative Identity Theft: Criminalizing Deepfakes Using the Right of Publicity*, IdeaExchange@UAkron.

[6] *Lawfulness of the Mass Processing of Publicly Accessible Online Data for the Development of Generative AI*, *International Data Privacy Law*.

[7] *Digital Identity: An Approach to Its Nature, Concept, and Functionalities*, *International Journal of Law and Information Technology*.

[8] European Data Protection Supervisor, *TechDispatch #3/2025: Digital Identity Wallets*.

[9] OECD, *Navigating the Next Ten Years of Digital Identity: Implementing Chile's National Digital Identity Strategy*.

[10] Atlantic Council, *Trustworthy Digital Identities Can Set the Standards for Secure Benefits Provision in the US*.

[11] *A Global Digital Identity for All: The Next Evolution*, Taylor & Francis.

[12] Stanford HAI, *Privacy in an AI Era: How Do We Protect Our Personal Information?*

[13] Lohsse, S., Schulze, R., and Staudenmayer, D. (eds.), *Data as Counter-Performance: Contract Law 2.0?* Nomos, 2020.

[14] *Data as Counter-Performance – Contract Law 2.0? An Introduction*, ResearchGate.

[15] *Data as Counter-Performance and Transformative Contract Law*.

[16] *Paying with Data: A Study on EU Consumer Law and the Protection of Data-Paying Consumers*.

[17] *Gaps and Opportunities: The Rudimentary Protection for Data-Paying Consumers under New EU Consumer Protection Law*, Kluwer Law Online.

[18] BEUC, *Assessment of Meta's Latest Pay-or-Consent Policy for Facebook and Instagram Users*.

[19] *The Pay-or-Consent Model and Competition Policy: A Case Comment on the European Commission's Decision Against Meta Under the Digital Markets Act*.

[20] *Meta's Pay-or-Okay Model: An Analysis under EU Data Protection, Consumer and Competition Law*, *Technology and Regulation*.

[21] Paul, Weiss, *How Does Data Regulation Interface With Antitrust Considerations? The European Data Protection Board Calls for Close Cooperation*.

[22] *The EU Artificial Intelligence (AI) Act: An Introduction*, ResearchGate.

[23] European Data Protection Board, *Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models*.

[24] Future of Privacy Forum, *Red Lines under the EU AI Act: Understanding Prohibited AI Practices and Their Interplay with the GDPR and DSA*.

[25] Wiley Rein, *Deepfakes, Deep Claims: Using Intellectual Property to Combat Artificial Intelligence's Digital Deception*.

[26] Jones Walker, *Deepfakes-as-a-Service Meets State Laws: Governing Synthetic Media in a Fragmented Legal Landscape*.

[27] Brookings Institution, *Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth*.

[28] *Digital Inheritance and Regulatory Gaps: The Post-Mortem Management of Personal Data Between Private Autonomy and Platform Power*, ResearchGate.

[29] *Digital Assets and Inheritance Law: Legal Vacuum or New Paradigm.*

[30] *Post-Mortem Privacy and Digital Legacy: A Qualitative Enquiry*, ResearchGate.

[31] *Exploring Swedish Perceptions on Post-Mortem Digital Data Management: Insights into Digital Legacy and Stewardship.*

[32] OpenID Foundation, *The Unfinished Digital Estate.*

[33] Harbinja, E., *Digital Death, Digital Assets and Post-Mortem Privacy.* Cambridge University Press, 2021.

[34] Rothman, J. E., *The Right of Publicity: Privacy Reimagined for a Public World.* Harvard University Press, 2018.