

## **Foundation of the Principles of Individual Digital Sovereignty**

### **Preliminary Note on Conceptual Scope**

The use of the term Individual Digital Sovereignty in this manifesto is not intended to replace, deny or dispute the sovereignty of the State in the classical legal-political sense. It is used as a doctrinal category intended to describe a strengthened sphere of personal self-determination in the face of the informational power exercised by public and private actors in the digital society.

Individual Digital Sovereignty does not propose absolute individual power, unlimited proprietary ownership over all information related to a person, or a form of anonymity immune from the law. Its primary foundation is dignity, autonomy, personality, freedom and effective control over the uses of digital identity that may affect a person's rights, opportunities or conditions of life.

This manifesto argues that identification, authentication, attribute verification and access to personal information must be subject to criteria of legality, necessity, proportionality, minimisation, transparency, responsibility and due process. The protection of digital identity does not require isolating the individual from the law, but rather preventing participation in the digital society from depending on the permanent, unnecessary or disproportionate exposure of the person.

Accordingly, this proposal does not seek to replace existing frameworks for data protection, privacy, identity or technological responsibility, but to highlight the need to evolve from a model centred primarily on the processing of data towards a model centred on the person as the holder of a digital identity deserving of reinforced protection.

### **Introduction**

Humanity is facing a transformation comparable to the great changes that defined the Modern Age and the Industrial Revolution. For centuries, individual freedom was linked to control over one's own body, private property and participation in public life without arbitrary subjection. However, the twenty-first century has introduced a new dimension of human existence for which our legal, economic and political institutions were not designed: digital identity.

Every search, movement, conversation, purchase, social interaction or expression of opinion may generate information capable of being stored, analysed, correlated and exploited on a massive scale. The accumulation of these data has produced an unprecedented concentration of knowledge about individuals and has given rise to a new form of power based on the ability to observe, profile, predict and influence human behaviour.

Information has become one of the most valuable strategic resources of our era. Personal data feed artificial intelligence systems, advertising markets, digital platforms, financial infrastructures and automated decision-making mechanisms. Yet those who continuously generate that value rarely exercise effective control over it and, in most cases, do not participate meaningfully in the benefits, decisions or conditions arising from its exploitation. This asymmetry has altered the balance between individuals, institutions and organisations. The more society depends on data, the less real capacity many people have to control the information that describes them. The more valuable digital identity becomes, the more urgent it is to recognise mechanisms capable of protecting personal autonomy against systems able to classify, condition or influence human life.

For this reason, privacy can no longer be conceived solely as a defensive right aimed at concealing information. It constitutes an indispensable condition for individual freedom, moral autonomy, human dignity and the effective exercise of fundamental rights in the digital age. When a person loses control over the information that represents them, they do not lose privacy alone: they lose decision-making capacity, bargaining power, self-determination and freedom.

This manifesto maintains that the time has come to recognise a new generation of digital rights capable of restoring the balance between individuals and institutions, returning effective control over digital identity to persons, and ensuring that technological transformation continues to serve human freedom rather than erode it.

## **I. Digital Identity Is an Extension of the Person**

Digital identity is not merely a set of technological records. It represents the projection of human personality in the digital environment.

Digital attributes, credentials, interactions, reputation and informational footprint form part of the contemporary representation of the individual. Therefore, digital identity must receive legal protection equivalent to that granted to other fundamental elements of personality. No person should lose effective control over the digital representation of themselves.

## **II. Data Concentration Generates Power Concentration**

Personal data are currently one of the most valuable resources in the global economy. The massive accumulation of information makes it possible to build detailed profiles, anticipate behaviour and exert influence over individual and collective decisions. When control over such data is concentrated in a small number of actors, power is also concentrated. Digital inequality does not arise solely from differences in access to technology, but also from differences in access to the knowledge derived from data. The defence of privacy is therefore a defence against excessive concentration of informational power.

## **III. From Data Protection to Individual Digital Sovereignty**

Individual Digital Sovereignty is the legal, technical and institutional capacity of a person to exercise effective control over their digital identity, limit its exposure, revoke authorisations, demand transparency and participate in decisions that affect their digital representation.

Recent decades have witnessed important advances in the legal protection of privacy and personal data. Regulatory instruments such as the European Union's General Data Protection Regulation have strengthened the rights of persons in relation to the processing of personal information by public and private organisations. The recognition of rights such as access, rectification, erasure, objection, restriction of processing and portability constitutes one of the most significant developments in the contemporary evolution of digital rights. However, data protection and individual digital sovereignty are not equivalent concepts. Data protection establishes limits on how third parties may collect, use and store personal information. Individual digital sovereignty, by contrast, requires the person to retain an effective capacity to decide over the digital identity that represents them in the technological environment.

Despite regulatory advances, the dominant model of the Internet continues to rely on architectures in which users' identity, personal attributes and data are stored, managed and exploited mainly by organisations that control platforms, services and digital infrastructures. In practice, the individual often exercises rights over information that has already been collected, stored and processed by third parties.

The next stage in the evolution of digital rights requires a shift from a paradigm centred exclusively on data protection towards a paradigm centred on the person. Individual digital sovereignty does not require eliminating organisations as custodians or processors of information, nor does it prevent the legitimate exchange of data. Its purpose is to rebalance the distribution of informational power, ensuring that the person retains effective control over the digital elements that constitute or affect their identity.

This sovereignty implies, at a minimum, the capacity to know what information exists about oneself, determine who may access it, decide for what purpose it may be used, establish temporal limits, revoke authorisations, transfer attributes between systems and demonstrate only those attributes strictly necessary for a legitimate digital interaction.

Data protection was a necessary response to the challenges of the information society. Individual digital sovereignty represents the next step in the evolution of fundamental rights for a society defined by artificial intelligence, the data economy and digital identity.

#### **IV. Fundamental Definitions**

To delimit the scope of this proposal, this manifesto uses the following concepts in the sense set out below.

Digital identity means the set of attributes, credentials, identifiers, records, interactions, reputation, metadata, inferences and representations that make it possible to describe, recognise, classify or link a person in digital environments. It is not reduced to an account, a username or an electronic document, but constitutes an informational projection of the person.

A digital attribute means any characteristic, condition, quality, authorisation, capacity, relationship or verifiable datum associated with a person in the digital environment, such as age of majority, residence, a qualification, a licence, institutional affiliation or a specific authorisation.

A verifiable credential means a digital statement issued by a competent or recognisable entity, capable of being checked by third parties, through which a person may prove an attribute, right, condition or qualification without revealing more information than necessary.

Personal data means any information that identifies, describes, affects or may reasonably be linked to a natural person, whether directly or indirectly, including information provided, observed, recorded, generated, correlated or processed based on their activity.

Inferred data means any information, prediction, classification, assessment, profile or conclusion produced about a person through the analysis of other data, even where that person has not directly provided such information.

A digital profile means any structured, total or partial representation of a person built through personal data, observed data, inferred data, behavioural patterns, algorithmic assessments or statistical correlations, capable of influencing decisions that affect that person.

Exposure of identity means the disclosure, communication or making available of elements that allow a person to be identified, recognised, tracked or linked in each context.

Identification means the process by which it is determined or confirmed who a person is. Authentication means the process by which it is verified that a person is who they claim to be or that they control a given credential, account, device or access method. Attribute verification means the process by which a specific characteristic is proven without necessarily revealing full identity.

Custody of personal data means the position of responsibility assumed by any organisation, entity or system that requests, stores, processes, retains, analyses or allows access to personal information. It entails proportional duties of justification, security, minimisation, traceability, confidentiality, accountability and reparation.

Individual digital sovereignty means the legal, technical, practical and institutional capacity of a person to exercise effective control over the elements that constitute their digital identity, determine the legitimate conditions of its use, limit its exposure, revoke authorisations, demand transparency and participate fairly in decisions that affect the digital representation of themselves.

Value generated by personal data means the economic, strategic, organisational, predictive, advertising, technological or commercial benefit that an entity obtains through the systematic collection, analysis, inference, aggregation, exploitation or monetisation of information linked to persons. Recognising this value does not mean reducing human dignity to a commodity, but requiring mechanisms of justice, control and responsibility.

## **V. The Right to Verifiable Identity and Minimal Exposure**

Democratic societies require spaces in which people can express themselves, participate and relate to others without being subjected to the permanent and unnecessary exposure of their identity. At the same time, digital coexistence requires mechanisms that allow responsibility to be attributed when unlawful, abusive or contrary-to-public-interest conduct occurs.

For years, the debate on identity on the Internet has been presented as a choice between absolute anonymity and permanent identification. Both models are insufficient. Absolute anonymity may make it difficult to attribute responsibility; permanent identification, on the other hand, forces people to expose personal information to organisations that do not always need to know it and are not always prepared to safeguard it adequately.

The need to identify a person where there is legitimate cause and proper procedure does not mean that the person must permanently reveal their full identity in all digital interactions. One of the fundamental errors of contemporary digital architecture is to assume that identification and exposure are inseparable. They are not.

An advanced digital society must be able to verify identities, attributes or credentials without requiring constant exposure of identity.

Just as a person can prove that they are of legal age without revealing all the information contained in their identity document, they should also be able to prove residence, professional status, possession of a credential or the condition of being a real person without unnecessarily exposing their name, address, identity documents or other additional data.

The principle is clear: no person should be required to reveal more information about themselves than is strictly necessary to participate in a legitimate digital interaction. Exposure of identity must be minimal, controlled and proportionate to the purpose pursued.

Contemporary technology already makes it possible to build systems based on verifiable credentials, cryptographic proofs and attribute validation that significantly reduce the need to share personal information. The central question is no longer only technical, but legal, political and social.

The objective is not to eliminate responsibility or prevent the legitimate action of authorities where necessary. The objective is to ensure that participation in the digital society does not require a disproportionate renunciation of privacy and control over one's own identity. The digital freedom of the twenty-first century will depend on our capacity to build systems in which people can be identifiable when necessary but not permanently identified by default.

## **VI. Legitimate Limits, Safeguards and Due Process**

Individual Digital Sovereignty is not an absolute right and cannot be interpreted as a barrier against every legitimate form of identification, investigation, supervision or regulatory compliance. The reinforced protection of digital identity must coexist with legal certainty, the protection of third parties, fraud prevention, the prosecution of unlawful conduct and the legitimate public interest.

However, the existence of legitimate purposes does not by itself justify the permanent, indiscriminate or preventive exposure of people's identity. The possibility of identifying a person where there is legitimate cause does not require all people to remain permanently identified, traceable or exposed in every digital interaction.

Any limitation on Individual Digital Sovereignty must be subject to strict criteria of legality, necessity, proportionality, specific purpose, minimisation, independent oversight and due process. Forced identification, access to personal information, disclosure of sensitive attributes or intervention over digital credentials should only be permitted where there is a sufficient legal basis, a clearly determined legitimate purpose and effective safeguards against abuse.

Legitimate identification must be distinguished from generalised surveillance. One thing is to allow a competent authority, under lawful conditions and adequate safeguards, to attribute responsibility for unlawful conduct. It is quite another to impose digital architectures that require the constant, unnecessary or disproportionate disclosure of full identity.

Privacy, pseudonymity, minimal exposure and informational autonomy do not protect fraud, harassment, extortion, identity theft, exploitation of minors, unlawful manipulation, abusive discrimination or other conduct contrary to the dignity, security or rights of other persons.

Similarly, sovereign digital identity systems must not lead to a single mandatory identity, a universal traceability infrastructure or a centralised mechanism that enables the systematic surveillance of a person's activity across different areas of life.

For this reason, every legal or technological architecture inspired by Individual Digital Sovereignty must incorporate mechanisms of control, review, challenge, traceability and reparation. The person must be able to know when their identity or attributes have been accessed, by whom, for what purpose and under what legal basis, except in legally justified exceptional cases subject to appropriate supervision.

The purpose of this manifesto is not to weaken the rule of law, but to prevent the digital society from confusing responsibility with total exposure. Digital freedom requires legitimate and proportionate mechanisms for attributing responsibility, without imposing permanent identification by default.

## **VII. The Economic Value of Digital Identity and Fair Participation in Its Benefits**

The contemporary digital economy rests on a continuous flow of information generated by billions of people through their daily activities. Every interaction, search, movement, purchase, publication, connection or behavioural pattern may contribute to datasets that feed artificial intelligence systems, digital platforms, advertising markets, financial infrastructures and predictive models of enormous economic value.

However, there is a profound asymmetry between those who continuously generate information and those who possess the technological, legal, economic and organisational capacity to transform it into value.

Individuals constantly contribute to the digital ecosystems that enable the creation of wealth, but the benefits derived from the collection, analysis, inference, aggregation, training, profiling and monetisation of that information are concentrated mainly in the organisations that control the infrastructures and systems of data exploitation.

This situation raises a fundamental question of justice, autonomy and distribution of power in the digital society. If digital identity is an extension of the person, and if information linked to that identity systematically contributes to the generation of economic value, it is not legitimate for individuals to remain structurally excluded from all capacity for decision, control, negotiation or participation in relation to the benefits obtained from their information.

However, participation in the value generated by personal data must not be understood as a simple sale of privacy or as a reduction of human dignity to a commodity. The person must not be forced to sell exposure, intimacy or vulnerability to participate in the digital economy. A truly free society must not build markets in which those with fewer resources are pushed to surrender more personal information in exchange for immediate economic advantages.

For this reason, recognition of the economic value of digital identity must be framed in terms of justice, governance and responsibility, not the absolute commodification of the person. The issue is not to affirm that every personal datum has a directly calculable individual price, nor to attribute absolute proprietary ownership over all information involving a person.

Many data are relational, inferred, aggregated, derived or produced within complex systems.

The central question is different: when an organisation obtains economic, strategic, predictive or commercial value systematically from information linked to persons, there must be mechanisms that guarantee transparency, control, equity, accountability and, where appropriate, fair forms of participation, compensation or equivalent benefit.

Fair participation in the value of personal data must be especially cautious where it affects persons in situations of vulnerability, minors, workers, dependent consumers, migrants, persons with disabilities, patients, users of essential services or groups exposed to intense forms of profiling. In such contexts, the formal capacity to accept an economic exchange does not necessarily guarantee a free, informed or fair decision.

Individual Digital Sovereignty requires the simultaneous recognition of two ideas. The first is that personal information cannot be treated as a free, unlimited and permanently available raw material for economic extraction. The second is that the dignity, privacy and identity of the person must not be reduced to tradable assets governed solely by price, contract and formal consent.

The challenge of the digital society is not simply to pay for data, but to redesign the distribution of power, control and benefits arising from the systematic exploitation of personal information.

### **VIII. Duties of Organisations, Safeguards and Remedies**

Recognition of Individual Digital Sovereignty would lack effectiveness if it were not translated into concrete duties for organisations that request, collect, store, process, analyse, infer, share or monetise personal information. Digital rights cannot depend solely on abstract declarations or on the individual capacity of each person to confront deeply asymmetric legal, technical and economic systems.

Every organisation involved in the processing of information linked to a person must assume, at a minimum, a duty of justification, minimisation, security, traceability and accountability.

No personal datum should be requested, retained or processed without a specific, legitimate, comprehensible and proportionate purpose. Where a digital interaction can be carried out through verification of a specific attribute, full exposure of identity should not be required.

Custody of personal data must entail a standard of protection proportionate to the sensitivity, volume, purpose and risk of the information processed. The greater the risk that data collection creates for the person, the greater the responsibility of those who decide to collect, retain or exploit it.

Organisations that use automated systems, artificial intelligence models, profiling mechanisms or algorithmic decisions that may significantly affect a person must assume reinforced duties of transparency, explanation, review and challenge.

The person must not be reduced to a passive object of classification, prediction or automated decision-making without an effective possibility to understand, question or correct its effects.

A duty of effective revocability must also be recognised. Where a person has authorised the use of certain data, attributes or credentials, they must be able to withdraw that authorisation in a simple, comprehensible and proportionate manner, without artificial obstacles, abusive penalties or designs intended to hinder the exercise of their rights.

Individual Digital Sovereignty also requires a duty not to exploit informational asymmetries. Organisations must not take advantage of technical complexity, dependence on a service, lack of real alternatives or user vulnerability to obtain consent that is formally valid but materially unbalanced.

Where these duties are violated, effective remedies must exist. Depending on the nature and seriousness of the case, such remedies may include clear information about the violation, rectification, erasure, restriction of processing, revocation, suspension of abusive uses, portability, human review, independent audit, proportionate compensation and sanctions where there is negligence, abuse or serious non-compliance.

Reparation must not be limited to administrative fines.

Where a violation of digital identity, privacy, data custody or minimal exposure causes real harm or significant risks to a person, the system must provide accessible, swift and effective avenues for complaint.

Likewise, the protection of Individual Digital Sovereignty requires institutional safeguards: competent authorities, oversight mechanisms, complaint procedures, audits, technical standards, documentation obligations and forms of independent control capable of preventing these principles from being reduced to voluntary commitments without consequences.

The legitimacy of an organisation in the digital society must not be measured only by its capacity to innovate, scale or generate economic value, but also by its capacity to respect the identity, autonomy, privacy and dignity of the persons whose data make its activity possible.

## **IX. The Relational and Collective Dimension of Digital Privacy**

Individual Digital Sovereignty takes the person as the centre of protection, but it must not be understood as an isolated or purely individualistic theory. In the digital society, personal information rarely exists in complete separation. Many data are relational, shared, inferred or derived from interactions involving several people, communities, organisations or social contexts.

A conversation, a photograph, a shared location, a contact list, a professional relationship, a communications history or a set of genetic data may reveal information not only about one person, but also about third parties. Likewise, algorithmic profiles built from certain individuals may be used to infer characteristics, risks or behaviours of other persons or similar groups.

For this reason, individual control over personal data must coexist with duties of respect for the privacy, dignity and rights of other persons. No one should be able to invoke their own digital sovereignty to unjustifiably expose another person's information, disclose shared data without regard for third parties or facilitate forms of collective profiling that generate discrimination, surveillance or exclusion. Digital sovereignty must also recognise a collective dimension.

Certain practices of data collection, inference, profiling or monetisation may affect not only specific individuals, but also groups, communities or categories of persons.

In areas such as artificial intelligence, targeted advertising, scoring, predictive surveillance, recruitment, credit, insurance, health, education, migration or essential services, data-based decisions may reproduce inequalities, amplify biases or generate significant consequences for persons who do not even know the origin of the inferences that affect them.

For this reason, Individual Digital Sovereignty must be complemented by principles of relational responsibility and collective justice. Organisations must respond not only for the processing of identifiable data relating to a specific person, but also for the aggregate, inferential or collective effects that their systems may produce on groups of people.

Recognition of this dimension does not weaken the centrality of the person. It strengthens it. A serious theory of digital identity must protect the individual without ignoring that data circulate, combine, are interpreted and produce effects within complex social systems.

## **X. Principles of Individual Digital Sovereignty**

Individual Digital Sovereignty is grounded in a set of guiding principles intended to inform the design of technologies, regulatory frameworks, identity infrastructures, governance models and organisational practices in the digital society. Their common purpose is to preserve dignity, autonomy, freedom and the person's effective capacity for decision-making in the face of informational power.

### **1. Principle of the Centrality of the Person**

Every digital architecture that collects, processes, infers, shares or monetises personal information must begin from the premise that the person is not a mere source of data, an exploitable profile or a passive object of algorithmic classification.

### **2. Principle of Sovereignty of Identity**

Every person must retain a primary sphere of decision-making over the attributes, credentials, identifiers, representations and elements that constitute or affect their digital identity.

### **3. Principle of Effective Control**

Every person must have legal, technical and practical means to know, authorise, limit, revoke, transfer, correct, challenge or prevent certain uses of the data, attributes and credentials that affect their digital identity.

### **4. Principle of Reinforced Informational Self-Determination**

Every person must be able to know, understand and decide how the information that describes them is used, especially when it is employed to profile, classify or influence them, or to make decisions that affect their rights, opportunities or reputation.

### **5. Principle of Minimal Exposure of Identity**

No person should be required to reveal more information about their identity than is strictly necessary for a legitimate digital interaction. Whenever it is possible to prove a specific attribute without exposing full identity, the least intrusive solution must be preferred.

### **6. Principle of Proportionality and Specific Purpose**

Any collection, access, retention, inference, communication or exploitation of personal information must respond to a legitimate, specific, comprehensible and proportionate purpose.

### **7. Principle of Transparency, Explainability and Traceability**

Systems that collect, process, infer or use personal information must operate in a comprehensible, verifiable and auditable manner. The person must be able to know what information is used, for what purpose, by whom, for how long and with what relevant effects.

### **8. Principle of Responsibility and Custody**

Every organisation that requests, stores, processes, infers, shares or monetises personal information assumes a duty of custody proportionate to the sensitivity, volume, purpose and risk of the data processed.

## **9. Principle of Revocability and Effective Reparation**

Any authorisation relating to the use of personal data, attributes or credentials must be revocable in a simple and effective manner, unless there is a legitimate legal basis to the contrary. Any significant violation must give rise to accessible, proportionate and effective remedies.

## **10. Principle of Portability and Interoperability**

Every person must be able to transfer their attributes, credentials and personal information between systems, platforms, organisations and jurisdictions without losing control over them or being subjected to artificial technological dependencies.

## **11. Principle of No Mandatory Centralisation**

Individual Digital Sovereignty must not lead to a single, mandatory, centralised or universally traceable digital identity. Identity systems must allow separation of contexts, legitimate pseudonymity and protection against generalised surveillance.

## **12. Principle of Inclusion, Accessibility and Usability**

Individual Digital Sovereignty will only be real if it can be exercised by any person, regardless of age, educational level, economic condition, disability, language, migration status, digital literacy or access to advanced technology.

## **13. Principle of Fair Participation in the Value of Data**

Where personal information systematically generates economic, strategic, predictive or commercial value, there must be fair mechanisms of transparency, control, governance, compensation, participation or equivalent benefit.

Every technology, regulation, public policy, digital identity infrastructure or business model based on personal data should be evaluated considering these principles.

## **XI. Towards a Charter of Rights for Individual Digital Sovereignty**

Technological transformation has profoundly altered the way people identify themselves, relate to others, work, access services, participate in public life and are evaluated by public and private institutions.

Just as political, industrial and constitutional revolutions gave rise to new generations of rights, the digital revolution requires an updating of the legal framework designed to protect human freedom, dignity and autonomy.

This proposal maintains that every person should be recognised as the holder, at least, of the following fundamental digital rights. These rights must not be understood as absolute or isolated from the rest of the legal order. Their exercise must be articulated in accordance with the law, the protection of third parties, legal certainty, the legitimate public interest, proportionality, specific purpose, minimisation and due process.

### **1. Right to Sovereign Digital Identity**

Every person must retain a primary sphere of decision-making over the attributes, credentials, identifiers, representations, reputation, data and elements that constitute or affect their digital identity.

### **2. Right to Effective Privacy**

Every person must be able to participate in the digital society without being subjected to permanent surveillance, disproportionate collection of information, unnecessary exposure of identity or processing incompatible with their dignity, autonomy and fundamental rights.

### **3. Right to Verifiable Identification with Minimal Exposure**

Every person must be able to prove attributes, rights, conditions or credentials necessary for a legitimate digital interaction without revealing more personal information than is strictly necessary.

### **4. Right to Reinforced Informational Self-Determination**

Every person must be able to know, understand, decide, limit and revoke the use of the information that describes or affects them, especially when it is used to classify, profile or influence them, or to make relevant decisions.

### **5. Right to Protection against Abusive Inferences and Profiling**

Every person must be protected against opaque, disproportionate, discriminatory or purpose-incompatible inferences, profiles, predictions, assessments or classifications capable of producing significant effects on their life, rights or opportunities.

## **6. Right to Algorithmic Transparency and Meaningful Explanation**

Every person must be able to know when a relevant decision affecting them has been adopted, influenced or conditioned by automated systems, algorithmic models or artificial intelligence systems, and to receive comprehensible information about their general logic, purpose, data used, effects and avenues for challenge.

## **7. Right to Human Review and Challenge of Automated Decisions**

Every person must be able to request human review, raise objections, provide context, correct information and obtain an effective response when an automated or algorithmically assisted decision produces significant effects on their rights, opportunities, reputation or living conditions.

## **8. Right to Universal Portability of Identity, Data and Attributes**

Every person must be able to transfer their credentials, attributes and personal information between platforms, organisations, services and jurisdictions without losing control over them or being subjected to artificial technological dependencies.

## **9. Right to Effective Revocation**

Every person must be able to withdraw previously granted authorisations for the use of their data, attributes or credentials in a simple, comprehensible and effective manner, unless there is a legitimate legal basis justifying their retention or processing.

## **10. Right to Responsible Custody of Personal Data**

Every person has the right to require organisations that request, store, process, infer, share or monetise personal information to adopt measures proportionate to the sensitivity, volume, purpose and risk of the data processed.

## **11. Right to Traceability and Accountability**

Every person must be able to know, in clear and accessible terms, what information is retained about them, who has accessed it, for what purpose, for how long, under what legal basis and with which third parties it has been shared, except for legally justified and supervised exceptions.

## **12. Right to Effective Reparation**

Every person must have access to accessible, swift and effective avenues for complaint in response to violations of their digital identity, privacy, minimal exposure, informational self-determination, data custody or rights in relation to automated systems.

## **13. Right Not to Be Subjected to a Single Mandatory Digital Identity**

Every person must be protected against systems that impose a single, centralised, universally traceable digital identity necessary for all forms of social, economic or political participation.

## **14. Right to Inclusion, Accessibility and Usability**

Every person must be able to exercise their digital rights regardless of age, language, educational level, economic condition, disability, migration status, digital literacy or access to advanced technology.

## **15. Right Not to Be Exploited through Informational Asymmetries**

Every person must be protected against practices that exploit technical complexity, dependence on a service, lack of real alternatives, contractual opacity, manipulative design or user vulnerability to obtain formally valid but materially unbalanced consent.

## **16. Right to Participate Fairly in the Value Generated by Personal Data**

Where personal information systematically and predictably generates economic, strategic, predictive or commercial value, persons must have access to fair mechanisms of transparency, control, governance, compensation, participation or equivalent benefit.

These rights do not seek to replace the fundamental rights recognised by contemporary legal systems. Their purpose is to extend, deepen and adapt those rights to a reality in which digital identity, personal data, verifiable attributes, algorithmic systems and the information economy have become essential elements for the effective exercise of human freedom.

The Charter of Rights for Individual Digital Sovereignty must not be conceived as a closed catalogue, but as a doctrinal basis for the legal, technical and institutional evolution of the rights of the person in the digital society.

## **Conclusion**

The fundamental question of our time is not only who owns technology, but who exercises the power derived from information. The digital revolution has given rise to a particularly profound form of power: the capacity to collect, retain, analyse, infer, profile, predict and exploit information about the lives of millions of people.

In this context, digital identity has become an extension of the person. Personal data, verifiable attributes, credentials, interactions, reputation, metadata, profiles and algorithmic inferences may condition the way in which a person is recognised, assessed, classified, accepted, excluded, surveilled or influenced by public and private systems.

Freedom in the digital age does not depend solely on access to technology. It depends on each person's real capacity to retain control over the identity that represents them, the information that describes them and the systems that may affect their rights, opportunities and conditions of life.

The digital society will not be truly free while participation in economic, social, cultural and political life requires the permanent and unnecessary exposure of identity. Nor will it be fully just while those who generate the value that feeds the data economy remain excluded from all capacity for decision, control, governance, reparation or participation in relation to the benefits derived from that exploitation.

The defence of individual digital sovereignty does not require isolating the individual from the law or denying legitimate purposes of identification, security, fraud prevention or protection of third parties. It requires that identification not become permanent exposure; that responsibility not turn into generalised surveillance; that innovation not justify unlimited data extraction; and that formal consent not conceal structurally unequal relationships.

The next evolution of fundamental rights must not be limited to protecting data as isolated objects. It must protect persons

against the forms of power exercised through data. It must recognise digital identity as part of the sphere of individual autonomy, require responsible custody, guarantee minimal exposure, subject automated systems to accountability and provide effective remedies when digital identity is violated.

The defence of privacy is, ultimately, a defence of human freedom. The defence of digital identity is a defence of human dignity. The defence of individual digital sovereignty is a defence of each person's capacity to remain their own master in the age of data, without being reduced to a profile, product, prediction or exploitable resource.

The history of fundamental rights has been the history of the progressive expansion of freedom in the face of new forms of power. Individual digital sovereignty is a proposal to continue that history in the era of artificial intelligence, the data economy and digital identity.

## About This Document

This manifesto is a foundational document for the development of a legal, technological, social and philosophical theory of Individual Digital Sovereignty. Its purpose is not to offer a definitive regulation, a closed legislative proposal or a single technical solution, but to establish the principles, concepts, rights, duties and safeguards that should guide the protection of the person in the era of digital identity, artificial intelligence and the data economy.

Individual Digital Sovereignty is formulated here as a doctrinal category intended to expand and deepen existing frameworks of data protection, privacy, identity, transparency, technological responsibility and fundamental rights. It does not seek to replace those frameworks, but to identify their structural limits and propose an evolution towards a model in which the person occupies the centre of the digital ecosystem.

This document should be understood as an intellectual foundation open to development, criticism and improvement. Its full development will require a later work analysing its historical, philosophical, legal, technical and institutional foundations, as well as its risks, limits, objections, implementation mechanisms and forms of protection, reparation and governance.

London, June 2026

J.C. Roura

Author of the Foundation of the Principles of Individual  
Digital Sovereignty

Foundational Version 2.0