



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE SOVEREIGN SELF: OWNERSHIP RIGHTS AND DIGITAL PERSONHOOD IN THE AGE OF THE DIGITAL TWIN

~ NEILOTPLA PALAK

ABSTRACT

This paper explores the far-reaching legal, philosophical and geopolitical challenges that have arisen with the emergence of Human Digital Twin (DT) technology. This study challenges the historically dominant yet conceptually problematic metaphors of data extraction, and introduces the Digital Twin as a symbiotic extension of human identity, as a "Digital Personhood" that is a manifest instance of a person. We construct a dangerous legal asymmetry between the authors of computational architectures and the inventors of human behavioural essence through a synthesis of technical architectures, the IP "stack" and geopolitical theories of strategic autonomy. We examine the evolution of digital twins from the simple to the autonomous, prescriptive and how this is an assault on individual cognitive liberty and free will, as digital twins continue to evolve and become more powerful, with ever-increasing levels of real-time, automated feedback and simulation of human behaviour.

This paper is a powerful proposal for "Data Dominion" which treats the unauthorized creation or manipulation of a human replica as identity theft, not just property infringement, and makes it lawful. Lastly, we suggest some practical remedies that can be implemented in today's jurisprudence, and use a Notice of Motion as a tool to enforce statutory "kill switches" under the General Data Protection Regulation (GDPR) and the sanctity of the In 1991, computer

scientist David Gelernter described a paradigm shift ¹in human-computer interaction that would soon come to pass in his influential book *Mirror Worlds: The Parallel Universes of Computer Simulation and Reality*.

The rise of software systems that would encapsulate, synchronize and operate large-scale, real-time simulations of the physical world. Gelernter predicted that these “mirror worlds” would one day break out of their institutional confines and become “multi-layered and dynamic” dimensions of the digital world that would coexist with humans. The term “Digital Twin” was introduced in 2010 in the aerospace industry in the context of optimizing the physical-model simulation of complex spacecraft systems, by NASA engineer John Vickers.² The classical digital twin architecture was established by Dr. Michael Grieves and is based on a triad: a physical object in real space, a virtual representation in digital space and a continuous communication channel—the “digital thread”—providing a two-way flow of information.³

I. INTRODUCTION

Digital twin is not limited to industrial systems, civil infrastructures and supply chain logistics, but has entered the realm of human simulation, which has caused a deep ontological crisis. Over the past almost 20 years, corporate, legal and economic models have considered personal data from the perspective of the consumer, under the frameworks of property and transaction. Historically, data was viewed as an outside, passive, and passive resource, a shared asset that could be harvested, sold and maximised by institutional players.

These extractive approaches are explicitly rejected in this paper. When continuously aggregated, synchronized and animated by powerful machine learning models, personal data stops being a mere trace of the past and starts reflecting the living, predictive image of human consciousness, biology and behaviour. The human Digital Twin is a “symbiotic system,” a legal concept coined by Marina Teller, which resides on the edge between personhood and property, and challenges the legal doctrine of identity. Thus, the present legal situation is a critical juncture. The high fidelity, human digital twins are challenging the jurisprudence of privacy, which has traditionally meant the right to be left alone, into a new jurisprudence of Digital

¹ David Gelernter, *Mirror Worlds: The Parallel Universes of Computer Simulation and Reality* (1991).

² Nat'l Aeronautics & Space Admin., *Draft Modeling, Simulation, Information Technology, and Processing Roadmap*, Technology Area 11 (2010) (co-authored by John Vickers, formally introducing the term into the agency's foundational space technology milestones).

³ Michael Grieves & John Vickers, *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*, in *Transdisciplinary Perspectives on Complex Systems* 85, 87–93 (Franz-Josef Kahlen et al. eds., 2017).

Human Rights. If the law does not change, then the individual will be structurally separated from their virtual image and the monopolies of the companies will take over the behavioural, psychological and physical templates of human beings.

The human Digital Twin is an inalienable extension of the “Sovereign Self” that must be recognised in law, this paper argues. In order to substantiate this claim, it is necessary to delve into the technical architectures that connect the virtual copy to the physical person, to break down the shortcomings of the existing IP regime, to examine the systemic societal dangers of automated simulation and to explain procedural legal remedies that can establish individual data dominion in an increasingly algorithmic world.

II. TECHNICAL ARCHITECTURE AND ONTOLOGICAL TAXONOMY: FROM PASSIVE SHADOWS TO AUTONOMOUS REPLICAS

In order to build a legally robust defence of the Sovereign Self, the technical mechanisms that enable digital twinning of a human being must first be broken down. One of the biggest errors made by modern-day regulators is to confuse a Digital Twin with the previous generations of technology: the digital model and the digital shadow.

It is well known in the systems engineering literature that a digital model has no automatic exchange of data with its physical model, and a digital shadow has one way data flow with changes in the physical object being reflected in the digital object, but not the other way around.

A real Digital Twin, on the other hand, involves a continuous, dynamic and bidirectional communication loop.⁴ The closed-loop architecture is key to the systemic integrity of a digital twin, as real-time behavioural data, physiological biometrics and contextual inputs are recorded by pervasive sensor networks (wearables, environmental IoT, mobile tracking interfaces) and sent via ultra-low latency networks to the virtual environment as shown by Maggie Mashaly. There, the input data stream is fed into advanced computational models which perform predictive simulations and send optimization commands or subtle feedback cues back to the physical entity, in real-time, directly changing its operational or behavioural state.

This technical taxonomy can be further elaborated by aligning human twin development with technological institutions' maturity models, such as IBM's⁵. This existential risk of the digital

⁴ Maggie Mashaly, *Connecting the Twins: A Review on Digital Twin Technology & its Networking Requirements*, 184 *Procedia Comput. Sci.* 299 (2021).

⁵ IBM Think Topics, *What Is a Digital Twin?*, IBM (2025)

twin to human free will and cognitive liberty grows in direct proportion to its place along this evolutionary maturity continuum:

➤ **DESCRIPTIVE TWIN (DIGITAL TWIN PROTOTYPE - DTP)**

This basic level contains snapshots of the past, individual consumer data, and static consumer profiles. It is the 'look-alike' stage of simulation. Although it can be used to describe the behaviour of the past, it does not have the infrastructure to support live synchronization, and does not adapt to the real-time changes of the environment of the individual and his psychology.

➤ **THE DYNAMIC TWIN (DIGITAL TWIN INSTANCE - DTI)⁶**

At this stage of maturity, the twin is directly connected to one particular person in the human life, and is so connected throughout the life of that person. With continuous data synchronization across the digital thread, the DTI integrates real-time health data, heart-rate variability, spatial location and continuous neural-linguistic outputs. This live data is then used to build a very individual predictive model that can anticipate the response of this individual to the current external stimuli, environmental changes or physiological stressors.

➤ **AUTONOMOUS TWIN (DIGITAL TWIN AGGREGATE TO AUTONOMOUS EXECUTION)**

The most advanced level of digital twin maturity involves advanced reinforcement learning, predictive analytics, and autonomous reasoning engines [3, 9]. At this level the human twin is not just a mirror or a prediction, but it is also an independent entity that performs continuous "what if" simulations in a virtual environment, which is not directly accessible to the human consciousness.

The Autonomous Twin can simulate millions of different combinations of environmental, informational and sensory inputs to produce a highly specific, pre-determined behavioural output from the physical human twin.

This advanced symbiosis requires an infrastructure with zero latency data transmission, edge-cloud synchronization and algorithmic opacity. The low latency requirement emphasized by Mashaly is no longer just an engineering measure but an unprecedented means of structural

⁶ Michael Grieves, Virtually Perfect: Driving Innovative and Lean Products through Product Lifecycle Management 205–12 (2011) (defining the "Prototype" as the generic template and the "Instance" as the individual, telemetry-linked asset).

control in critical human domains like personalized medicine, remote neural monitoring and cognitive behavioural tracking.

The two-way feedback loop can be used as a weapon, if an autonomous corporate twin can process an individual's biometric stress signals and simulate his/her cognitive weaknesses quicker than the person's own conscious mind can register them. The free will is effectively put under the control of the predictive optimization of a proprietary algorithmic model [3, 4].

III. "TO BE" VERSUS "TO HAVE": THE ONTOLOGICAL CRISIS

The autonomy of the human twin, the bilateral nature of the operation and the human nature of the twins inevitably raise a deep philosophical and legal question, the essence of which is captured in Marina Teller's words: "To Be" vs. "To Have"⁷. It is a dichotomy which smacks of the very core of Western liberal jurisprudence, which is essentially split into two fundamental categories: persons (the subjects of rights, as they are) and things (the objects of rights, as they are owned).

According to the classical legal principles, man is a person without a doubt, he is. Corporate enterprise, on the other hand, aims for the Digital Twin to be placed firmly in the realm of property, which a commercial enterprise can have. The corporation's rationale is based on a narrow materialistic, technological argument: the virtual model is an artificial asset, the only property of the corporation, because these assets were created by the corporation, stored on its own cloud servers and the capital was invested in their construction by the corporation itself. But this property-centric approach fails when it comes to the special case of human data synchronization. A digital twin cannot be separated from the actual exploitation of the physical person's biological and behavioural nature, which makes it functional, predictive and its form itself. The twin is not a separate program that simply characterizes an external object but is an active, digital part of the unique personhood of the individual, which is alive and alive in itself, is in constant motion and is subject to life processes.

The law in its corporate "To Have" structure tacitly legitimizes a very risky legal position. The legal system allows the creation of a tradable and severable corporate asset from an individual's behavioural and biological identity, effectively stripping the individual of his/her own digital identity. This estrangement opens the door to what can be called Biometric Capitalism, a socio-economic system in which companies are able to buy, sell, lease, or modify the virtual copies

⁷Marina Teller, *L'avatar juridique*, 1 Revue des Droits de l'Homme 145 (2021)

of human beings, and use them to generate economic value or test new and intrusive behavioural interventions without the subject's awareness or systemic consent.⁸

In this automated world, the law must strongly support the "To Be" paradigm and take the human Digital Twin as an integral part of Digital Personhood that can never be separated from it. In this sense, the virtual clone is considered an analytical surrogate of the human soul, a technological representation of the integrity of the body and mind of each person. Therefore, the rights of the twins are not rights that can be alienated, waived or captured by corporations, but rather fundamental, inalienable human rights which are permanently attached to the physical sovereign to whom they belong.

IV. THE INTELLECTUAL PROPERTY PARADOX AND STRUCTURAL ASYMMETRY

The limitations of the law in respect of the protection of the Sovereign Self are due to a structural crisis of the international Intellectual Property Rights (IPR) regime. The individual who tries to take control of his/her digital twin is confronted by a multi-layered "IP stack", which is optimized to secure the corporate capital rather than his/her identity.

This proprietary corporate stack is normally divided into three separate legal protections. This is a very strong structural imbalance, this traditional legal system:

1. THE COPYRIGHT LAYER

The user interface of the digital twin is made up of specific 3D visual representations or "skins" that are copyrighted by corporations, as are the application programming interfaces (APIs) and underlying source code. Even if the twin's voice, facial movements and idiosyncratic gestures are a perfect copy of the voice of a real person, the legal system will protect the software rendering of the voice of the person of the corporation.

2. THE PATENT LAYER

The machine learning workflows implemented, the predictive control loops and the real-time data processing techniques for synchronizing the twins are described by wide-spread corporate

⁸ Margaret Hu, *Biometric Surveillance Capitalism*, 62 B.C. L. Rev. 2453, 2455–60 (2021).

patents. In many countries including India (Indian Patents Act 1970) there are still many ambiguities about the patentability of software or computer programs as such.⁹

However, technology firms are constantly finding ways to overcome these limitations by patenting such systems as a complete, industrial “technical application” or hardware-software “ecosystem” and therefore gaining control over the infrastructure of human simulation.

3. THE TRADE SECRET LAYER

The vaguest is the trade secret protection. Mathematical weights, hyperparameters and matrices that change during the processing of an individual's behavioural data in the deep neural network are kept secret and proprietary, as if they were trade secrets. This results in an algorithmic "black box" that no one can audit, challenge or comprehend how it is simulating their identity.

Such a legal structure is a basic paradox: the owner of the platform enjoys full legal protection for the vessel, whereas the owner of the essence is left completely exposed. The classical principles of property law are not at all appropriate to this tension, which has arisen in the context of non-replicable, discrete tangible property.

The digital twin is a mix of human spirit and company's code, a company that has patented algorithms to capture an individual's biometric data flow. The law is what it is and tech monopolies have an implied right of eminent domain over human identities, can block interoperability between platforms, and can restrict the individual's ability to control their own simulated futures.

V. SOCIETAL RISK AND ALGORITHMIC SUBJUGATION: THE SIX DIMENSIONS OF THREAT

The legal status of digital twins is not only a theoretical problem, but a practical one that threatens the stability of democratic societies and the integrity of the individual's mind. The systematic presentation of the usage of the advanced digital twins in computer science literature shows high risks of privacy, security and management.

1. THE DATA PRIVACY DIMENSION

The traditional point-in-time consent measures are redundant because a true digital twin can only be truly in sync with a high-fidelity stream of behavioural data that it receives over time.

⁹ The Patents Act, No. 39 of 1970, § 3(k), India Code (1970) (*incorporating the Section 3(k) software exclusion recommendation*).

The person is constantly being observed and recorded by the state, and all of their physiological changes, objects they look at in their unconscious state and micro-transactions are also recorded in order to maximize the virtual model. It makes the difference between public and private interiority totally redundant.

2. THE "FAKE TWIN" PROBLEM AND THE DATA SECURITY DIMENSION

The technical attack surface of digital twins is growing exponentially as they become more and more complex, making them highly vulnerable to data security. One of the main threats mentioned in the literature is the development of "Fake Digital Twins". Malicious users or a competitor or adversarial company may be able to insert data into the digital thread or create a copy of a specific user's algorithm.¹⁰

These systems are two-way, and a rogue or armed "Fake Twin" can then send spoofed commands back to the real person, altering his access to smart-home systems, his dosing of medicine, or even engage in identity theft on a systemic level on a scale never before seen.

3. THE DATA MANAGEMENT DIMENSION

Data in the digital thread is a regulatory concern that is not addressed. The data lineage is lost when an individual's twin is spread out over edge devices, cellular relay stations and centralized cloud servers.

Who is in control of the life cycle of the simulation? Does the individual's digital twin become a liquidated asset to be auctioned off to the highest bidder if a corporation goes bankrupt? There is no explicit management standard and hence human identity is regarded as a transient data packet that floats in an unmanaged corporate ether. The Infrastructure and Standardization Dimension is the fourth dimension. The fourth dimension is Infrastructure and Standardization Dimension.

Today, the digital world is completely devoid of universal technical standards and cross-platform interoperability. Digital twin architectures are deliberately made incompatible by large technology monopolies, thus resulting in a walled garden. This digital infrastructural division closes the individual's digital personhood in the private network of the corporation. It

¹⁰ Fei Tao et al., *Digital Twin Security: A Survey and Analysis of Vulnerabilities, Threats, and Defenses*, 18 IEEE Trans. Indus. Informatics 7623, 7625–30 (2022) (detailing cybersecurity attack vectors where malicious or altered bidirectional telemetry returns harmful commands to physical systems or subjects).

is hard to move health and psychological dual from one tech company's platform to another tech company's platform, thus establishing a new form of digital serfdom.

4. THE PATENT LAYER

The machine learning workflows applied, the predictive control loops and the real-time data processing techniques for the synchronization of the twins are protected by wide-spread corporate patents. There are still many uncertainties regarding the patentability of software or computer programs as such in many countries such as India (under the Indian Patents Act 1970).

But tech giants regularly work around these limitations by patenting these systems as complete, industrial “technical applications” or hardware-software “ecosystems,” and thus controlling the infrastructure of human simulation.

5. THE TRADE SECRET LAYER

The least clear element of the stack is trade secret protection. The mathematical weights, hyperparameters and matrices that are updated in the behavioural data of an individual while the data is being processed by a deep neural network are considered trade secrets and are kept confidential. This results in an algorithmic "black box" that no one can audit, challenge or comprehend how it is simulating their identity.

This legal form is a classic contradiction: The owner of the platform is fully protected by the law, while the creator of the essence is completely vulnerable. The classical principles of property law were not at all appropriate to this tension, being developed to resolve tension in the case of discrete, non-replicable tangible property.

The digital twin is a blend of human spirit and business code—a business entity that is able to record the flow of biometric data of an individual through its patented algorithms. The law stays the same, and tech monopolies have an implicit right of eminent domain over human identities, can block interoperability between platforms, and can restrict the individual's ability to control their own simulated futures.

6. LEGAL AND SOCIAL DIMENSION

Last but not least, the legal and social aspect reveals the complete lack of legal and social frameworks governing "Virtual Identity". Who is liable if an autonomous digital twin, which

exists independently within a corporate network, makes a financial transaction, produces a defamatory output or fails to fulfil a contractual obligation in a virtual space?

Jurisprudence is currently woefully short of an understanding of digital inheritance and immortality. When a physical individual dies, does their "live" predictive digital twin stay owned by the tech firm, so that the tech firm can continue to profit from a "ghost bot" of the deceased indefinitely? If digital persons are not legally recognised, society will be completely chaotic, with the living and dead being both commodified by autonomous software engines.

7. INFRASTRUCTURE AND STANDARDIZATION DIMENSION

There are no universal technical standards and there is no interoperability across different platforms in the contemporary digital landscape. The walled garden is a digital twin architecture intentionally designed by large technology monopolies to be incompatible with other architectures.

This digital fragmentation of infrastructure entices the individual's digital identity into private corporate networks. The seamless transfer of an individual's health or psychological twin from one ecosystem that is owned by one of the technology giants to one owned by another is not a possibility, and thus there is a new kind of digital serfdom.

VI. STATUTORY LEVERS AND PROCEDURAL REMEDIES: THE JURISPRUDENCE OF THE NOTICE OF MOTION

We need to look to practical procedural tools that can challenge corporate power in court to make the Sovereign Self a legal reality and bring it from the philosophical realm to the practical. Theory of human rights is of little use without the effective and timely procedural instruments. The main defence tool in modern civil law that will be useful to a defence attorney to defend a person from an unauthorized algorithmic replication is the Notice of Motion.

A Notice of Motion is, in the digital twin exploitation context, a modern-day writ of Digital Habeas Corpus, a document that makes a demand to a company to "produce the body" of the virtual twin for judicial review, audit and structural repair. If an attorney finds that a tech company has built an unauthorized predictive model of a client, he or she should file a motion for urgent interim relief with the court.

The immediate goal of the motion is to obtain an injunction to stop the "digital thread" in its tracks, to prevent the flow of data going both ways and to prevent the corporate from sending out autonomous control signals or predictive nudges to the physical individual.

In order to meet the rigorous requirements of the law for granting interim relief, the moving party is required to prove three elements of civil procedure:

- **PRIMA FACIE CASE:** Counsel must establish a clear, legally protected right to data dominion, showing that the corporate entity has built a high-fidelity simulation model of the unique biological or behavioural essence of the applicant without clear and unambiguous consent, in a structurally mannered way.
- **BALANCE OF CONVENIENCE:** The harm that is being done to an individual when their cognitive liberty and privacy is permanently lost as a result of an autonomous corporate twin that is going to cause a short-term financial inconvenience to a tech company must outweigh that inconvenience.
- **IRREPARABLE INJURY:** Most importantly, counsel must prove that the applicant would suffer irreparable harm if the court were not to grant the applicant immediate interim relief to freeze the data loop. Since autonomous twins are always running and the latency is negligible, an unvetted simulation running without restraint will cause an irreversible dilution of identity that is hard to compensate for later with monetary damages.

The necessary statutory basis needed to ensure that this Notice of Motion has real enforcement power is already there in advanced international frameworks, such as the General Data Protection Regulation (GDPR). ¹¹Litigators can make the compliance with GDPR a shield for Digital Personhood by explicitly linking a Notice of Motion to the codified provisions of the GDPR.

There are four key statutory levers to a strong, strategic movement:

1. THE RIGHT TO ERASURE

If the individual is moved by a Notice of Motion, then Article 17 gives him an absolute legal "kill switch". Once a person formally withdraws consent from the simulation, the court may exercise this statutory authority to issue an injunction that forces the corporation to remove the

¹¹ Regulation 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

Digital Twin Instance (DTI) from its servers and delete all of the behavioural telemetry and untether the digital thread without "undue delay".¹²

2. THE ARTICLE 20 LEVER (THE RIGHT TO DATA PORTABILITY)¹³

Article 20 is a strong countermeasure to vendor lock-in and corporate digital serfdom. It provides the data subject with the right to obtain their personal data in a structured, commonly used and machine-readable format and to transmit their personal data to another controller without any restriction.

A Notice of Motion can be used in a digital twin dispute to force a corporation to provide the full computational architecture of a client's twin, and move it into an independent and secure personal data vault where the individual has sovereign control over their virtual profile.

3. RIGHT TO PROTECTION AGAINST AUTOMATED PROFILING (ARTICLE 22)¹⁴

Article 22 clearly states that the right to not be subjected to a decision based exclusively on automated processing, including profiling, which affects them in a legally significant way or significantly affects them. This article is the main statutory protection from the systemic threats of predictive discrimination.¹⁵

If a Notice of Motion is brought to move any sort of corporate or institutional action including automated adjustments to healthcare access, credit scores, and employment opportunities that is based on the virtual simulations of an autonomous twin then counsel may invoke Article 22 to obtain a stay on such action. It compels the institution to give up the automated mirror and to go back to the transparent and human processes.

¹² Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, paras. 70–85 (establishing the benchmark parameters for requiring digital architecture operators to permanently expunge personal profiles that undermine identity and privacy rights)

¹³ Regulation 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), art. 20, 2016 O.J. (L 119) 1 [hereinafter GDPR].

¹⁴ GDPR art. 22, para. 1.

¹⁵ Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 Colum. Bus. L. Rev. 494, 501–15 (2019) (evaluating how automated profiling under GDPR Article 22 addresses the legal limits of drawing predictive, highly invasive conclusions about human behavior).

4. LEVER 25 (DATA PROTECTION BY DESIGN AND BY DEFAULT)¹⁶

Article 25 takes the focus of litigation from reactive to proactive, from litigation to technical architecture. It has a legal requirement for software developers and platform creators to embed data protection principles and individual rights into the very engineering of the system, from the first line of code.

A digital twin action may require a company's computational models to be audited to ensure they meet the requirements of Article 25. If the system is not technically able to isolate an individual's data, it has no encrypted enclaves, or it would not be possible to make an instant “kill switch” to shut down a digital twin across the entire digital thread, then the court can enjoin the deployment of the entire digital twin infrastructure, declaring it to be illegally designed by default.

VII. GEOPOLITICAL SCALABILITY: STRATEGIC AUTONOMY AND THE NEW DIGITAL HUMANISM

The susceptibility of the person to corporate algorithmic capture does not just extend to the micro level of domestic law, but also to the macro level of international relations and global geopolitics. The problem takes a very different form when multi-national technology monopolies have the infrastructure to build fully formed, independent predictive twins of entire populations, and it's no longer an individual problem of identity theft, but a problem of state sovereignty and national security.

The traditional understanding of sovereignty, which has long been based on physical geography, militarized borders and kinetic power, is rapidly changing as analysed by ¹⁷geopolitical scholar Paul Timmers. Today, when simulation is everywhere, a nation-state's strategic autonomy – its ability to regulate its own technology, defend its critical infrastructure and ensure the security of its citizens' collective data – is becoming the defining factor of its sovereign integrity as it is becoming increasingly dependent on foreign technology monopolies and cyber-adversaries.

As Timmers points out, digital sovereignty has emerged as one of the international conflict zones. When a country opens up the behavioural, physiological and psychological data of its

¹⁶ GDPR art. 25.

¹⁷ Paul Timmers, *Sovereignty in the Digital Age*, in Introduction to Digital Humanism 401, 401–405 (Hannes Werthner et al. eds., 2024).

entire population to be freely exported to foreign artificial intelligence laboratories or to be hosted on foreign cloud architectures, the country is effectively experiencing a modern-day Digital Colonization.¹⁸

A foreign power or an overseas corporation with an Autonomous Twin of an entire nation can run large-scale “what if” scenarios to determine the vulnerabilities of a nation's economy, simulate civil unrest and carry out highly targeted cognitive warfare operations to disrupt and topple democratic elections well before the physical nation can respond with a counter-strategy. Nation-states are thus being called upon more and more to play a macro-stewardship role in the world, with data localization policies and tight regulatory control serving as a new technological battleground. The idea of a national digital twin, like the United Kingdom's Gemini Principles framework, which seeks to achieve a 'synchronised model of national infrastructure', shows that states see digital twinning as an important instrument for the public good¹⁹. But to maintain national strategic autonomy, governments should also give this protection to their populations' biological and behavioural twins. Today, the collective digital personhood of a country is becoming an important leverage in international diplomacy and a strong negotiating tool. Like trade embargos or resource limitations in the past, today's sovereign states are increasingly limiting the movement of citizens' biometric and neural data across borders.

States are leveraging data dominion, requiring foreign AI companies to build local data centres, submit weights of their neural networks to national data audits, and adhere to strict national digital personhood regulations. This State-level intervention is a line of defence to prevent the emergence of a borderless, stateless, algorithmic feudalism in the digital thread which connects a population to technology, and is subject to democratic accountability and sovereign law.

VIII. CONCLUSION

The technology and growth of human Digital Twin is a new paradigm shift in the development of our digital civilization. The legal frameworks of the past, which saw personal data as an external and passive good, are completely outdated. As we have shown in a detailed analysis of technical, philosophical and legal aspects, the human Digital Twin is not a product for sale,

¹⁸ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* 112–125 (2023).

¹⁹ Centre for Digital Built Britain, *The Gemini Principles: Guiding Values for the National Digital Twin* 6–12 (2018), https://www.cdbb.cam.ac.uk/files/the_gemini_principles.pdf.

but a living, dynamic and symbiotic part of the human identity, a technological representation of the Sovereign Self.

To overcome the deep systemic conflicts between the designer of the computational platform and the inventor of the human substance, a radical departure from the classical approach to property rights and a bold step into the jurisprudence of Digital Human Rights is needed. The need for an immediate formulation of a New Social Contract, based on the fundamental principle of Data Dominion is demanded. In this new social contract, it is necessary to establish in law the synthesis, the predictive profiling, and the manipulation of a human being's digital clone as a criminal offence of identity theft, and not merely a civil matter of intellectual property.

This legal battle is of the highest stakes. The international community must not allow the corporate "IP stack" to be more important than human personhood, otherwise we will enter a new era of total algorithmic feudalism, which will statistically predetermine human behaviour, extinguish cognitive liberty and turn the individual into a proprietary asset of a technological monopoly.

On the other hand, we can establish a strong claim for autonomy of individuals by using simple instruments such as Notice of Motion, and by invoking the strong powers of the frameworks such as the GDPR, which already exist in the statute books. The law should clearly state that the human Digital Twin is a person. The Sovereign Self must be the sole and undisputed owner of its virtual shadow, so that the future of technology is always to be used for the development of digital humanism, and the maintenance of human freedom.