

SPECIAL ISSUE ARTICLE

Statehood in the Age of Digital-Physical Simultaneity: A Comparative Inquiry into Dislocated Sovereignty

Mohammad Ghasem Tangestani¹  and Mahdi Moradi Berelian² 

¹ Associate Professor, International Law Department, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.

² Assistant Professor, Public and International Law Dept., Faculty of Law and Political Science, University of Mazandaran, Babolsar, Iran

Corresponding author: Mahdi Moradi Berelian; Email: M.moradib@umz.ac.ir

(Received: 22/10/2025 - Accepted: 08/02/2026)

Extended Abstract

Introduction and Research Problem

Modern state theory was built around a geography of power. Territory, population, institutions and enforceable law gave public authority a place from which it could be recognized, limited and challenged. This territorial grammar has not disappeared. States still legislate, tax, educate, register, police and adjudicate within borders. However, it no longer explains the whole field of public power. A growing part of authority now moves through data systems, digital infrastructures, platform design, cross-border cloud services, identity frameworks and algorithmic decision-making. The state may still make law in a territorial setting, while governance effects are produced in digital spaces that do not neatly correspond to territorial jurisdiction.

This transformation creates a difficulty for Public Law. Classical accounts of Sovereignty usually linked authority to a politically organized space. The state was imagined as the place where law, coercion, legitimacy and accountability came together. Digital Governance unsettles this image. Code, interfaces, databases, automated classifications and platform rules may shape

How to Cite: Tangestani, M. G., & Moradi Berekian, M. (2026). Statehood in the Age of Digital-Physical Simultaneity: A Comparative Inquiry into Dislocated Sovereignty. *State Studies*, 12(47), 69-92. <https://doi.org/10.22054/tssq.2026.89032.1739>



State Studies Journal © 2015 by Allameh Tabataba'i University is licensed under Attribution-NonCommercial 4.0 International.

the citizen's legal position before any court, ministry or official appears. The problem is therefore not merely technological. It concerns the legal meaning of statehood, the changing relationship between authority and place, and the position of the citizen in a world where Digital Space and physical territory coexist. Existing discussions of network governance, platform power and algorithmic regulation have identified parts of this transformation. However, they have not always offered a theory of the state that explains how Sovereignty continues, weakens, and reappears under these conditions.

Research Objective

The article develops the concept of Dislocated Sovereignty as a public-law vocabulary for this evolving condition. The argument is not that territorial Sovereignty has ended, nor that private platforms have replaced the state. Those claims are too broad to capture legal reality. The stronger and more precise claim is that the state now works under a double condition. It remains territorial in form, jurisdiction, and constitutional imagination, but many of the mechanisms through which it governs data flows, platform architecture, algorithmic classification, digital identity systems, and infrastructural control operate across, beneath, or beyond territorial borders. Dislocated Sovereignty names this tension between the state's continuing territorial presence and the increasingly non-territorial settings in which public power is exercised.

Incorporate specific policy challenges and opportunities arising from 'Dislocated Sovereignty,' illustrating how this concept informs legal reforms and governance strategies, thereby engaging policymakers more directly.

Research Method

The research is analytical, conceptual and comparative. Its conceptual frame draws on Public Law theory, political sociology and selected debates in the philosophy of Sovereignty. Historical and conceptual accounts of the modern state are used to reconstruct the classical relation between territory and authority. Institutional and network theories help explain how power is distributed among public bodies, private actors, technical systems and human-machine arrangements. Genealogical and spatial approaches are also used to show why authority cannot be understood only by locating formal institutions. The comparative part of the article is selective rather than exhaustive. France, the European Union and Iran are not treated as equivalent cases. They are examined because each reveals a different legal response to the same underlying problem. France represents a republican effort to bring platform power back under public authority, especially through dignity-based regulation and child protection. The European Union shows how a non-classical legal order can construct a form of digital Sovereignty through data protection, fundamental rights, and risk-based regulation of artificial intelligence. Iran illustrates a more difficult

sovereignty gap: inherited territorial authority remains strong, but Digital Governance is still marked by coercive platform control, fragmented administrative systems, and the absence of a fully developed theory of digital Public Law.

Research Findings

The article reaches five main findings. First, territory still matters, but it no longer exhausts the meaning of state authority. Borders continue to organize jurisdiction, institutional responsibility and political membership. At the same time, the actual routes of governance increasingly pass through technical, transnational infrastructures that are often privately designed or owned. This creates a gap between the legal locus of decision-making and the locus of its effects.

Second, law is losing part of its older visibility as the public language of authority. In digital environments, code, default settings, terms of service, access rules and automated classifications may influence behavior more directly than statutes or administrative regulations. This does not mean that law disappears. It means that Public Law must follow public power into databases, interfaces, portals, protocols and algorithmic systems.

Third, legitimacy is being displaced. In the classical model, legitimacy depended on constitutional authorization, representation, public reason and accountability. In platform environments, obedience often appears as user consent, interface dependence or infrastructural necessity. The user may seem to agree, but usually lacks any real capacity to negotiate the conditions of Digital Governance. This weak form of consent cannot replace public accountability.

Fourth, the citizen is increasingly positioned not only as a rights-holder, but also as a data subject, a platform user, and a digital addressee of public authority. This can improve access to services, but it can also lead to exclusion, opacity, and silent administrative harm when systems lack notice, human review, correction procedures, and effective remedies. Digital Citizenship therefore requires more than access to portals. It requires contestability, explanation, alternative routes, and legal protection against system-based errors.

Fifth, comparative experience shows that Dislocated Sovereignty can be managed in different ways. France uses republican authority and dignity-based regulation to extend public values into platform environments. The European Union uses data protection, fundamental rights and market access to build a rights-based model of digital Sovereignty. Iran, by contrast, faces the unresolved task of transforming territorial command into accountable digital state capacity. Without such a transformation, the state risks being strong in formal authority but weak in trust, legitimacy and digital public law.

Conclusion

Dislocated Sovereignty is not a technological slogan. It is a public-law problem. It does not ask us to abandon the territorial state. It asks us to rethink the legal imagination of the state so that authority, accountability and dignity can survive when public power operates through Digital Space, data systems and algorithmic infrastructures. The state in the digital age cannot be only a machine of command, filtering or surveillance. It must explain algorithmic decisions, protect the dignity of citizens' data, supervise platform power, provide remedies for digital exclusion, and preserve public reason in environments built for speed, prediction, and extraction.

For Iran, this problem is especially urgent. A state without a coherent theory of digital Public Law may swing between ineffective coercion and passive dependence on platforms. Dislocated Sovereignty offers a way out of that false choice. It invites a reconstruction of statehood around trust, legality, transparency, accountability, and Digital Citizenship. In this sense, the future of the state will not be secured by repeating inherited formulas of Sovereignty, but by building public-law institutions capable of governing non-territorial spaces without losing the public character of authority.

Keywords: Authority Theory, Digital Citizenship, Digital Governance, Digital Space, Dislocated Sovereignty, Public Law, State.

Introduction

In modern public law, the state has often been understood through geography. A state has territory, population, institutions and a legal order that claims jurisdiction within a defined space (Jackson, 2007: 23–28; Morris, 2002: 87–94). Territory still matters, but it no longer marks the whole field of public power. Digital governance changes this grammar without abolishing it. The state still taxes, educates, licenses, registers, polices and adjudicates within territorial boundaries. Yet many of these acts are now carried out through platforms, databases, cloud services, biometric systems, digital identities and algorithmic tools (Zuboff, 2019: 200–205; Yeung, 2018: 509–512). The question is no longer whether the state has territory, iwebert is whether the legal rules that govern persons within that territory can still match the actual reach of state power.

This condition may be described as digital-physical simultaneity. Public power remains territorially anchored, but many of its tasks are increasingly performed in digital environments that are not bounded by geography. The problem is not merely administrative. It concerns the basic idea of statehood. If governance is mediated through data flows and platform design, can we still think of the state as a centralized locus of sovereignty? What happens to accountability when a legal decision is shaped by technical design and infrastructure? How can legitimacy persist when consent often appears as a click, a default setting or compelled dependence on a system? Classical theories of sovereignty do not fully answer these questions. Hobbes’s *Leviathan*, Rousseau’s account of popular sovereignty, Kant’s juridical order, Weber’s account of legitimate domination and Schmitt’s decisionism all kept authority close to an organized political space (Hobbes, 1996: 118–122; Rousseau, 2002: 81; Kant, 2006: 93; Weber, 1978: 212; Schmitt, 2005: 7–12). Later theories of network governance and reflexive regulation have expanded the discussion, but they have not always addressed the legal implications of place itself (Mann, 2012: 5–9; Walker, 2003: 16–20). They often speak about the multiplication of actors without fully confronting the separation between the legal site of decision-making and the practical site of its effects.

This article uses the concept of dislocated sovereignty to describe this condition. Sovereignty still exists, and private platforms have not replaced states in the strict legal sense. The more difficult problem is that the state remains territorial while many of the matters it must govern are non-territorial, distributed and technologically mediated. Sovereignty is therefore not lost, but shifted, rearranged and sometimes weakened by the very infrastructures that now support public authority. The argument

proceeds in three stages. First, it clarifies the historical relationship between state authority and territory. It then examines how digital infrastructures disturb that relationship without eliminating the territorial state. Finally, it compares France, the European Union and Iran to show how different legal orders respond, or fail to respond, to the dislocation of sovereignty.

Methodology, Scope, and Contribution

The article adopts a theoretical and comparative approach. Its framework draws on political sociology and public-law theory. It understands the modern state as a form of authority historically associated with territory, while also recognizing that non-state actors, economic systems, ideological networks and administrative technologies have always existed alongside it (Mann, 2012: 5–9). Digital technology, therefore, does not create distributed power from nothing. It intensifies older dispersions of power and gives them new legal significance.

The comparative inquiry is selective rather than exhaustive. France, the European Union and Iran are examined because each offers a different response to the same underlying problem. France stands within a strong republican and territorial tradition. The European Union operates through supranational legality and fundamental rights. Iran begins from a more centralized understanding of public authority, yet it faces similar pressures from platforms, data systems and digital administrative tools.

The article makes a theoretical rather than technical contribution. It does not examine cybersecurity, data management or platform engineering as technical fields. Instead, it focuses on legitimacy, accountability, authority, citizenship and legal form. The central question is how the state can remain legally accountable when governing power is exercised through technical arrangements that are often presented as neutral, private or opaque (Buchanan, 2004: 118–123).

Theoretical and Epistemological Foundations

Digital governance is often presented as a change of tools. Paper files become databases, queues become portals, signatures become authentication codes, and administrative decisions become automated notifications. That view is not wrong, but it is too simple. Digital transformation also reshapes our understanding and exercise of authority. It affects our conception of public power (Lessig, 1999: 6; Yeung, 2018: 509–512). When a citizen walks into a government building, they know where the power lies. The desk, the official, the file, and the seal all belong to a recognizable administrative world. On the other hand, a

citizen who interacts through a platform has a different experience. A database, rule engine, outsourced software provider, public agency, private intermediary, or a combination of these could make the decision. The location of authority becomes less clear and accountability less straightforward. The law may still be there, but now other frameworks for governance are more pressing.

This context helps us understand what dislocated sovereignty means. The idea emerges from a crisis of explanation. The traditional territorial model does not cover the whole field of governance anymore. Public power now operates across various registers, including physical offices, national territories, transnational platforms, cloud infrastructures, data exchanges, and algorithmic environments. A theory of the state that looks at territory alone will fail to see much of what the state now does, and much of what is done in its name.

The Genealogy of the Modern State and the Unity of Place and Authority

The modern state was born with a sense of place. From the sixteenth and seventeenth centuries on, sovereignty was more and more thought of as authority in a well-defined territory. For Hobbes, *Leviathan* and the later constitutional state implied that public authority requires a bounded, identifiable domain (Hobbes, 1996: 118-122). Territory was not simply the limit of power. It made authority readable. It told officials where it could act, citizens to whom it belonged, and courts which law to apply.

Jackson describes sovereignty as an idea shaped by the continuing struggle to define ultimate authority within political communities (Jackson, 2007: 3-6). In the history of the modern state, as told by Quentin Skinner, political authority gradually disengaged itself from the individual body of the ruler and was attached to an impersonal public order (Skinner, 2014: 12). The legal consequence of this development, as Christopher Morris puts it, is that the modern state is a territorially organized institution whose jurisdiction and coercive capacity are bound to a population living within defined borders (Morris, 2002: 197).

This territorial form distinguishes the state from other forms of power. Economic actors can cross borders to discover opportunities. Religious or ideological movements can create institutions that cross territorial boundaries. Corporations and platforms can now organize action across continents. The uniqueness of state authority lies in its claim to a monopoly of control in a certain area. This is where Michael Mann's account of the independent power of the state comes in. The state is not just one of many organizations; it can impose its will over space and

regulate social life in ways that more diffuse powers cannot (Mann, 1984: 199).

But territoriality was never complete. Empires, trade systems, religious groups, diplomatic rights, and international organizations always made the concept of sovereignty more complex. What is new in the digital age is the ubiquity of this complexity. The challenges are no longer confined to exceptional situations such as wars, diplomacy, or international trade. They are now appearing in everyday tasks: identity checks, education platforms, health records, tax websites, welfare payments, police databases, and digital evidence. The territorial state continues to function, but its behavior is increasingly directed by systems that do not have their explanation in territory alone (Zuboff, 2019: 76-78; Yeung, 2018: 509-512).

The Digital Crisis of State Knowledge

Digital governance changes the scope of state action and the way the state sees society. The modern administrative state viewed society through files, offices, censuses, registries, maps, and bureaucratic classifications. The digital state, by contrast, imagines society as interoperable databases, predictive models, biometric templates, behavioral traces, and platform interactions. This shift matters because power follows knowledge, and what the state can see affects what it can govern.

Mann's broader history of social power demonstrates that states have always been embedded in networks (Mann, 2012: 5-9). But the digital turn makes those networks denser, faster, less visible, and more dependent on technical design. Zuboff's account of surveillance capitalism reveals how behavioral data can be a resource for prediction, modification, and control (Zuboff, 2019: 200-205). Similarly, Yeung's work on algorithmic regulation considers how automated systems can guide conduct without the open form of traditional legal command (Yeung, 2018: 509-512).

Neil Walker's concept of sovereignty in transition helps identify the institutional aspect of this shift. Sovereignty is no longer located in a settled locus. Walker (2003: 16-20) locates it in disparate legal, political, and technical fields. The state remains important, but it no longer has a monopoly on the conditions in which authority is generated. It has to negotiate with platforms, standards, protocols, databases, vendors, users, and transnational legal regimes.

The epistemological crisis is practical as well as conceptual. It is pragmatic because governments often have difficulty controlling the digital systems they rely upon. It is conceptual because the traditional legal categories confer authority on formal institutions, but the actual

decisions are made somewhere else. A citizen left out by an automated system does not regard this as a theoretical matter. For that citizen, the question is simple and urgent: Who made the decision? What is the legal basis for it? And where can it be challenged?

The Components of Dislocated Sovereignty

Dislocated sovereignty can be explained through three interrelated concepts. Each involves a different breakdown of the traditional relationship between territory, authority, and legal responsibility. We see, first, a partial disjunction of authority and place. Law grounds authority in territory, but its operational effects flow through data networks and algorithmic systems. The inability to locate power in a formal location can be explained through Foucault's concepts of the various spaces of power as well as Lefebvre's theory of space production (Foucault, 1986: 22–27; Lefebvre, 1991: 26–33). Digital infrastructures generate their action spaces. These infrastructures connect, filter, permit, prevent, and rank various forms of information and interaction. They do not just carry out state decisions; they help shape them.

The second proposition is pluralism in the areas of jurisdiction. A single act of governance can be local, national and transnational all at once. International standards can influence a digital identity system hosted on foreign infrastructure, accessed by citizens through privately designed interfaces but created under domestic law. One of the best examples of the data exchange infrastructure is the Estonian X-Road, which allows safe information exchange between public and private systems, including cross-border systems (E-Estonia, 2024, X-Road section). That is not the lesson all states should learn from Estonia. This situation means that the public authority becomes more and more dependent on the design of relations between institutions and infrastructures.

The third proposition is the institutional-algorithmic composition of authority. Modern authority is not merely a human choice plus technical assistance. Nor is it an actual machine rule, either. The result is a mixed arrangement in which legal mandates, administrative discretion, data categories, codes, interfaces, and institutional habits shape each other (Yeung, 2018: 515). When a welfare system, a tax portal, or a public employment database produces an outcome, the decision is not always easily assigned to one official or one line of law. This mixed authorship of public power is the starting point of dislocated sovereignty.

These propositions do not deny the state. They make it harder to evade public responsibility. Authority is public authority even when

exercised through digital systems if it affects rights, access, services or legal status. For that reason, the state must remain responsible for the systems it builds, buys, connects with and uses.

Formulating the Theory of Dislocated Sovereignty

In the modern tradition, sovereignty was organized around a familiar triad: territory, population, and effective authority (Nelson, 2006: 43-46). That triad still is relevant for recognition, constitutional identity, and jurisdiction. However, a data-driven order introduces another condition that public law cannot overlook: infrastructural control. A state that can organize, protect, and lawfully use data can govern effectively. A state that can control data without accountability may govern in a harmful way. Both scenarios are part of the same change in sovereignty, influenced by digital infrastructure and data relationships.

Dislocated sovereignty, therefore, avoids two tempting but incomplete stories. One is the story of decline: the claim that globalization, digital platforms, or artificial intelligence have brought sovereignty to an end (Held & McGrew, 2003: 51-53). The other is the story of continuity: the assumption that old territorial categories can absorb digital governance without theoretical adjustment. The first exaggerates the state's retreat. The second underestimates the extent to which authority is displaced by infrastructure and data relations. A better account sees sovereignty as being reconfigured, not simply lost or preserved.

Beyond the Territorial Geometry of Authority

Modern political thought has frequently portrayed authority in geometric terms. Rousseau's people govern themselves in a political body; Kant's juridical order is about relations between spatially organized states; and Hegel's state is the ethical actuality of a political community (Rousseau 2002: 81; Kant 2006: 93; Hegel 1991: 279). In each case, authority assumes a specific form. You can think of authority as existing within a specific domain.

Digital power changes that geometry. Lessig's claim that code regulates remains relevant because it indicates that the architecture of a digital environment can make some actions possible and others difficult, expensive, or impossible (Lessig, 1999: 6). Code does not ask where the border lies. A platform's ranking system, identity policy, or content moderation rule may impact citizens in one country without being authored by the legislature of that country or supervised by its courts

(Zuboff, 2019: 151–154). The issue is not the lack of governance. It is design governance.

The territorial state has a range of responses available: it can legislate extraterritorially, build domestic infrastructure, cooperate with other legal orders, regulate platforms by sanctions, or rely on blocking and filtering. Every response carries costs. Dislocated sovereignty asks which of these responses is defensible in public law and which merely substitute coercion for lawful authority.

Overlapping Spaces of Rule

Today authority functions through a set of overlapping spaces rather than a single public space (Mann, 2012: 122–124; Kalmo & Skinner, 2010: 17). A government platform can be funded by the state, programmed by a contractor, hosted on external infrastructure, accessed from private devices, and governed by technical standards developed elsewhere. In this kind of setting, the once clear distinction between public and private vanishes. A private actor can perform a public function. Private architecture can be dependent on a public body. A citizen may be lawfully governed by law but practically governed by interface.

Latour’s actor-network theory is useful, not because algorithms are legal persons but because it highlights the production of order through the associations between human and nonhuman elements (Latour, 2005: 69–73). Public law cannot stop at the minister, the statute or the agency. It must ask how the decision is assembled. Who defines the data categories? Who audits the model? Who controls the database? Who can correct an error? Who is answerable when the system harms a person?

From Concentrated Authority to Distributed Design

The modern state placed authority in recognizable institutions: parliament, cabinet, courts, ministries and administrative agencies. Digital governance does not make those institutions irrelevant, but it disperses part of their authority into design. Public power is increasingly exercised through technical arrangements that shape conduct before any formal legal dispute arises.

Design can govern quietly. A default setting may determine whether personal data is shared. A portal may decide whether a person can reach a service. A database may determine whether a legal status is recognized. The state must therefore be judged not only by what it commands, but also by what it builds, buys, connects and automates (Morris, 2002: 88–91). Public authority is now embedded in procurement contracts, interoperability standards, data-sharing protocols and interface design. All

of these require public-law scrutiny because they shape both state power and citizen rights.

From Identity Authority to Infrastructural Authority

For modern states, national identity, collective memory and constitutional symbolism are often important. These still count. However, digital authority increasingly relies on infrastructure: the ability to authenticate people, secure records, exchange data, maintain service continuity and protect citizens from platform dependency (Bennett Moses & Chan, 2018: 9). Gill's account of the modern state helps show how institutions survive by organizing their capacities and meanings (Gill, 2003: 112). The digital age links the technical capacity of the state directly to political trust because infrastructural capacity informs citizens' perceptions of state legitimacy.

Dislocated sovereignty is a matter of public law. It asks the question of how authority may be exercised by means of infrastructure without losing its legal character. It also questions how the state can govern platforms and algorithms without digital governance becoming a permanent state of exception.

Conceptual and Structural Consequences for Modern Legal Order

Every theory of sovereignty carries an image of the state, the law, and the citizen. Once authority becomes dislocated, all three images change. The change is not dramatic in the theatrical sense; it is often slow, administrative, and almost invisible. However, its legal consequences are serious.

The Changing Concept of the State

Classical state theory defined the state as people, territory, and authority, a triad that defined the public order from the Westphalian system to the modern nation-state (Jackson, 2007: 23-28). Through law, the state continues to govern the population within its borders. However, in the platform era, the state manifests itself in additional forms beyond traditional governance. It frequently collaborates with other powers. Google, Meta, Telegram and other such infrastructures are not legally sovereign. They have no political people, no constitution and no public accountability in the public-law sense. Yet they wield functional power over speech, visibility, identity, access, and economic opportunities. The work of Zuboff demonstrates how platform companies are able to transform behavioral data into predictions and influences (Zuboff, 2019: 112).

Their power is not territorial, but it is real. This situation is a crisis of representation. Morris (2002: 87-94) contends that the modern state is partly defined by its claim to represent a bounded political order. In digital governance, the state can no longer represent fully the space in which its citizens are governed. Citizens are still subject to domestic law, but they also live on private platforms, cross-border data systems and global technical standards. The legal territory of the state and the practical territory of power no longer correspond to each other.

Iran shows this mismatch in day-to-day administration. Digital systems are becoming more and more important to the state, as shown by Shad in education, Sib in health management, Sejam in financial identity, and the taxpayers' system in fiscal governance. These systems can help increase access and coordination. But they also breed uncertainty, dependence and exclusion when they lack clear legal standards, auditability, and remedies. Ahmadvand and colleagues note that governance networks in Iran have created new challenges for state coordination and public accountability (Ahmadvand et al., 2024: 40).

The Erosion and Return of Law

Law was the dominant public language of authority. It made rules, assigned powers, defined rights, and allowed citizens to challenge decisions. Digital governance does not eliminate the law but rather conceals it beneath the surface of decision-making. Code, platform rules, and automated classifications can impact life more directly than legal texts.

Lessig's discussion of code as regulation is still the clearest point of departure (Lessig, 1999: 6). Zuboff offers a bleaker picture of how digital systems can predict and determine conduct without the deliberative form of law (Zuboff, 2019: 173-189). In administrative settings, the problem is not only surveillance capitalism. It also involves the rise of rule-based systems. Access can be refused if the system fails to confirm the identity of a person, the portal fails to recognize his or her status, or a database fails to match records. Even if the issues are technical in nature, the resulting damage has legal consequences.

For instance, Iranian efforts like Pakna, Sejam, and the National Window of Smart Government Services suggest that public law needs to focus more on infrastructure. Where access to rights or services is dependent on digital systems, these must function within the rule of law, transparency, proportionality, corrective measures, and human review. Otherwise, the law risks becoming a mere facade for decisions made elsewhere.

The aim is not to pit law against technology. We should put technology back under legal discipline. The digital administrative system needs to have a legal basis, a clear purpose, accountable operators, audit trails, error correction procedures, meaningful notices, and accessible remedies. Without these protections, digital systems can turn arbitrary decisions into technicalities.

The Displacement of Legitimacy

Legitimacy in public law has usually been connected with constitutional authority, public reason, representation, and accountability. In platform environments, compliance takes a different form. Users accept terms, agree to settings, provide data, and change behavior to comply with interface rules. This phenomenon is often referred to as 'choice', but the choices are limited. It is almost always unavoidable and rarely negotiated. The analysis of the platform economy by Julie Cohen demonstrates that digital legal relations are as much subject to control structures as they are to formal consent. (Cohen, 2017: 153-175). This is why legitimacy can become displaced: authority becomes less about public trust and more about dependence, design, and inability to exit.

Another consent box does not establish legitimacy. A state that depends on platforms or algorithms must provide citizens with means to understand, contest, and correct digital systems. Explanation, participation, and dignity are not just nice-to-have values; they are necessary for lawful digital authority.

This issue is especially serious in Iran. The state can continue to try to impose its will upon citizens when they face filtering, surveillance, opaque systems, or unexplained administrative rejections, but it forfeits the public trust that legitimizes its authority (Salmani et al., 2024, p. 1410; Shafiei Alavija et al., 2025: 555).

Legal Order as a System of Effects

The contemporary legal order was organized by jurisdiction. A rule was part of a legal system; a court applied it, an institution enforced it, and a citizen knew to which authority to address it. Instead, digital governance frequently functions as a system of effects. What is important is not only which body has jurisdiction but also which actor can in fact influence behavior.

Walker's (2003) definition of sovereignty in transition is a state of plural, overlapping, and unsettled legal authority (Walker, 2003: 45-52). Latour's work aids in understanding the porous borderlines between state, market, society, and technology (Latour, 2005: 112). Platform governance

exacerbates this porosity. The same individual could hold multiple roles simultaneously. The governance framework includes terms of service, content policies, app store rules, payment infrastructure, data standards, and domestic regulations.

The result is not an absence of norms. It is a crowded field of norms with uneven accountability. Citizens may be subject to domestic law, platform rules, technical standards, and security decisions, with no clear hierarchy among them. In Iran, debates over filtering Telegram or WhatsApp show the limits of territorial control when the state lacks full authority over infrastructure, and citizens rely on global platforms for their social and economic lives. Official decisions may be made, but their effectiveness, legitimacy, and legal coherence are often weak.

Dislocated sovereignty changes public law from a focus on jurisdiction alone to an emphasis on effects. The crucial question becomes: Who has the practical capacity to shape the citizen's legal and social position, and what public-law duties follow from that capacity?

Table 1. Traditional Sovereignty and Dislocated Sovereignty: A Comparative Overview

No.	Conceptual Element	Traditional Sovereignty	Dislocated Sovereignty
1	Basis of authority	Territory, population, and effective authority within a defined domain.	Data flows, infrastructural control, and regulatory influence in spaces beyond borders (Zuboff, 2019: 151-154).
2	Institutional structure	The state is the central source of public authority.	A network of state institutions, platforms, algorithms, contractors, standards, and users (Latour, 2005: 68-89).
3	Relation to place	Authority tied to territorial jurisdiction.	Authority is partly place-bound and partly place-evading (Kalmo & Skinner, 2010: 17).
4	Relation to law	Text-based law is enacted and enforced through public institutions.	Code, interface design, and algorithmic systems operate beside formal law (Lessig, 1999: 6).
5	Instruments of control	Police, courts, bureaucracy, fiscal systems, and formal supervision.	Data infrastructures, authentication systems, access rules, automated classifications, and platform design (Bennett Moses & Chan, 2018: 9).
6	Scope of authority	Primarily domestic and territorially bounded.	Distributed across domestic, transnational, public, private, physical, and digital spaces.
7	Legitimacy	Constitutional law, representation, national	Trust, transparency, contestability, data dignity, infrastructural

No.	Conceptual Element	Traditional Sovereignty	Dislocated Sovereignty
		identity, and public accountability.	reliability, and rights protection (Gill, 2003: 112-115).
8	Position of the citizen	Citizen as a member of a territorial legal order.	Citizen as rights-holder, data subject, platform user, and digital addressee of public power.
9	Logic of governance	Hierarchical, centralized, and office-based.	Distributed, adaptive, data-driven, and often dependent on non-state infrastructures.

Comparative Reflections

Comparative constitutional law once focused mainly on parliaments, courts, cabinets, federalism, and separation of powers. Those questions are still important, but digital governance raises a prior question: Where is public power actually exercised? While a state can legislate within its territory, the practical conditions of speech, identity, access, and visibility may form elsewhere. A platform has the potential to impact citizens without being democratically answerable to them (Zuboff, 2019: 189-192). Though it appears to be just an administrative tool, the algorithmic system can have legally significant consequences. These shifts suggest that scholars must examine sovereignty in terms of both its effects and its formal location.

The comparison considers five questions on Iran, the European Union, and France. How do the various legal systems view the relationship between state and territory? Has it developed tools for managing digital spaces that are beyond normal territorial control? How does it legitimate its authority in algorithmic and platform environments? How does it address private actors operating without borders? Has thinking in constitutional or public law recognized the changing relationship between place and sovereignty?

France: Republican Authority in a Platform Environment

The French republican model has long placed emphasis on public authority. The state is not a manager of private interests; it is the public order of the nation, expressed in general law. This republican vocabulary offers France an original way of responding to digital platforms, as the question is not only a matter of regulating markets or protecting consumers but also of defending public values in a space that is shaped by private infrastructures that influence public life (Rousseau, 2002: 81).

A telling example is French Law No. 2020-1266 of October 19, 2020, on the commercial use of the image of children under 16 on online

platforms (Loi no. 2020-1266, 2020, arts. 1-3). The law targets the phenomenon of child influencers, especially on video-sharing platforms. It provides for authorization or a declaration for certain activities, it protects a part of the child's income, and it recognizes the child's interest in controlling digital exposure. In doing so, public authorities reintroduce a new platform practice into the legal vocabulary of child protection, labor regulation, and dignity.

The law is important for the theory of dislocated sovereignty because it makes platform activity a matter of public concern. It recognizes the child as a rights holder and pushes republican authority into a digital environment that cannot be contained by territorial presence alone. France thus translates sovereignty into protection, supervision and dignity instead of leaving the platform field to private ordering.

French data protection law and the Commission nationale de l'informatique et des libertes reinforce the same pattern. CNIL's 2019 fine against Google LLC for failures in transparency and valid consent was more than a technical sanction. It was a public claim that the global data power has to be subject to legal standards that protect persons in France and across the European legal space (CNIL, 2019, paras. 1-2; European Data Protection Board, 2019, para. 1). The case exemplifies the ability of territorial legal authority to influence actors whose operational power is transnational.

French constitutional review (Conseil constitutionnel, 2018, 1-8) has also treated the adaptation of domestic data-protection law to the GDPR as a matter requiring constitutional scrutiny of accessibility, competence, and fundamental safeguards. The French approach then combines a rights vocabulary with strong public authority. Its weaknesses are also apparent: dignity-based regulation can become paternalistic when protection is divorced from participation. However, the model demonstrates that sovereignty can be rebuilt on dignity and oversight of institutions instead of mere censorship or symbolic assertion.

The European Union: Dignity, Data, and Risk-Based Sovereignty

The European Union is a special case because it is already a post-classical legal order. It is not a traditional state or a loose international organization. It has survived for decades with divided authority, overlapping competences, and legal pluralism (Bickerton, 2012: 40-45). That is why the EU is in some ways better placed than many states to consider the dislocation of sovereignty. The Charter of Fundamental Rights of the European Union opens the rights architecture of the Union with human dignity. Article 1 states that dignity is inviolable (Peers &

Ward, 2004: 93). This concept is important in digital governance because dignity can be more than a moral principle. This provision provides a legal basis for limiting the reduction of people to data points, risk categories, or behavioral profiles.

The General Data Protection Regulation best exemplifies this approach. This principle also applies outside the borders of the Union when controllers or processors established outside the EU target or monitor the behavior of individuals within the Union (European Parliament and Council, 2016, art. 3; Kuner, 2017: 32). This extraterritorial reach is often referred to as regulatory power, but it is also a form of dislocated sovereignty. The EU does not establish legal authority by occupying space but by attaching obligations to data relations affecting persons within its protection.

The EU Artificial Intelligence Act, Regulation (EU) 2024/1689, applies the same logic to algorithmic systems, too. Its risk-based structure bans certain AI practices, imposes obligations on high-risk systems, and establishes transparency duties for selected uses of AI (European Parliament and Council, 2024, arts. 5-6, 50). The Act is important because it views AI as a public law issue, not just an innovation. We cannot leave systems affecting fundamental rights, safety, or equality to technical optimism or market self-regulation.

Therefore, the EU model is building digital sovereignty based on rights, risk, institutional coordination, and market access. Its authority is not based on traditional territorial boundaries but rather has a specific placement. It rests on a legal community, a rights order, and the practical ability to control access to a market. It makes the EU a powerful example of the juridification of dislocated sovereignty.

The EU model has its flaws too. Its regulatory architecture is dense, compliance can become bureaucratic, and ordinary users may still consider it difficult to understand or challenge automated decisions. That is why dislocated sovereignty should not look to the EU for a final solution or a success slogan. It should be read as an advanced experiment in reconstructing public authority where borders alone no longer do the work.

Iran: The Sovereignty Gap in Digital Public Law

Iranian public law continues to cling to a classical notion of sovereignty: centralized power, territorial integrity, and state command. But digital power is increasingly transmitted through communication and data, rather than institutional location per se (Castells, 2009: 125). This older model is now operating in a legal and policy environment it was not designed to

manage. That leaves a vacuum of sovereignty. The state claims authority over digital life but has not yet constructed a coherent public law framework that can unite authority and accountability, technical capacity and rights, and security and the dignity of citizens.

This gap is in two directions. On the one hand, the state often uses rigid instruments like filtering, blocking, and coercive platform control. These tools may be attempting to reclaim sovereignty, but they seldom address the fundamental issue. Without domestic trust, lawful options, transparent standards, and accountable institutions, coercive control could undermine legitimacy rather than reinforce authority (Salmani et al., 2024: 1410). The state must build trust to establish itself as a credible regulator and guardian of digital rights.

The second dimension of the gap is in public administration. The development of digital state capacity is visible in systems like Pakna, Sejam, Shad, Sib, the taxpayers' system, and the National Window of Smart Government Services. They can cut down on paperwork and improve coordination. But without clear legal foundations, transparent data practices, algorithmic auditability, complaint mechanisms, and remedies, they risk turning citizens into passive data subjects. Ahmadvand et al. (2024: 51) alert us to the unresolved epistemological and accountability problems in Iran's networked governance.

Official policy documents have started to address artificial intelligence governance, citizenship rights, transparency, and digital transformation. But these ideas tend to be declarative. They are not always translated into binding obligations. The policy statement of the Islamic Consultative Assembly Research Center on AI governance is an important sign that the issue has entered the policy agenda (Islamic Consultative Assembly Research Center, 2023, policy statement section). But the legal system still needs stronger rules on data protection, algorithmic transparency, administrative due process, and platform accountability.

So the problem for Iran is not only technological backwardness or reliance on platforms. It is legal and theoretical. The state has not yet created a language of digital public law that corresponds to its ambitions. It needs a framework that can explain when digital authority is legitimate, how citizens can challenge automated or system-based decisions, how public bodies can be held responsible for outsourced or technical infrastructures, and how platform regulation can be conducted without reducing digital citizenship to control.

A public law theory of dislocated sovereignty would enable Iran to escape the false choice between surrender to platforms or coercive

closure. Instead, it would ask, "How can the state build trustworthy infrastructure, protect data dignity, regulate platforms proportionately, secure effective remedies, and include citizens in the design of digital public services?" Without this change, the state runs the risk of being strong in command and weak in legitimacy (Shafiei Alavija et al., 2025: 555).

Discussion: Toward a Public Law of Dislocated Authority

The cases illustrate a common problem. Digital governance not only constrains sovereignty, but it also alters the conditions for the credibility of sovereignty. France responds with its republican authority and rules based on dignity. The European Union is tackling this with rights, data protection, and risk-based rules. Iran is still searching for answers, often pulled between coercive assertion and institutional incompleteness.

Such a public law of dislocated authority would have to start with six practical commitments. First, digital public power requires a clear legal basis. Any system affecting rights, benefits, identity, mobility, or access to services must be grounded in law. Before it begins to govern, its purpose, scope, operator, and legal effects must be clear.

Secondly, digital systems must be transparent from the viewpoint of public law. The affected person doesn't need to see each line of code but needs to understand why a decision was made, what data was used, who made it, and how it can be challenged.

Third, human review must always be present when digital systems have significant legal effects. Automation can help with administration, but it should not take away the chance of hearing, correction, and judgment.

Fourth, data dignity must be acknowledged as a constitutional and administrative value. Citizens should not be reduced to risk scores, incomplete records, or predictive profiles without safeguards. People's data is not simply a resource but a way the state interacts with legal identity.

Fifth, platform regulation should be reasonable and credible; states have understandable reasons to regulate platforms on children's privacy, national security, competition, or democratic discourse. But regulation loses credibility when it is unclear, excessive, or disconnected from rights.

Sixth, digital citizenship must be more than access to websites. It should include participation in the design of public systems, means to file complaints, alternative options for people excluded by technology, and solutions to harm caused by digital administration.

These commitments will not resolve all problems. However, they help prevent the use of dislocated sovereignty to justify state overreach or private control. The goal is to make public authority accountable, not louder.

Conclusion

The modern state was once understood as the institutional form of collective will, legal order and effective authority within territory. That image still matters. No serious theory of digital governance can ignore territory, jurisdiction or public institutions. Yet the state now acts in a world where authority is often mediated through data infrastructures, platforms and algorithmic systems that do not fit the older spatial grammar of sovereignty.

The concept of dislocated sovereignty captures this condition. It identifies the gap between the place where law is made and the digital environments where governance takes effect. It also explains why borders no longer guarantee authority, why platforms can exercise power without public legitimacy, and why legal systems must follow public power into code, data and infrastructure.

This is not an argument against the state. On the contrary, it takes the state seriously enough to insist on accountability. A state that governs through digital systems must be able to explain them. A state that depends on platforms must regulate them lawfully and openly. A state that collects and processes data must protect the dignity of the persons behind that data through robust legal safeguards. If public administration is automated, remedies, hearings and human judgment must not disappear.

The comparative analysis shows that there is no single model of digital sovereignty. France offers a republican approach centered on dignity and public oversight. The European Union provides a rights-based and market-supported model. Iran reveals the risks of a state that remains strong in territorial language but weak in the design of digital public law. For Iran, the issue is not merely to create platforms or control them. It is to build a legal framework capable of governing digital life through trust, transparency, accountability and citizenship.

The future of the state will not be secured by repeating inherited formulas of sovereignty. It will depend on whether public law can reconstruct authority in non-physical spaces: databases, interfaces, protocols, clouds, algorithms and digital identities. Dislocated sovereignty offers a framework for that reconstruction. It asks the state to remain public as its instruments become digital, to remain accountable as its

decisions become automated, and to remain committed to human dignity as governance is increasingly organized through data.

Acknowledgements

This study received no specific financial support. The authors are responsible for the arguments, translations, and interpretations presented in the article.

Conflict of Interest

The authors declare no conflicts of interest.

References

- Ahmadvand, D., Ghorbanizadeh, V., Alvani, S. M., & Hoseinpour, D. (2024). Epistemology and challenges of governance and policymaking networks. *Quarterly Journal of Administrative Law*, 11(37), 33-63. <https://doi.org/10.61186/qjal.11.37.33> [In Persian]
- Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society*, 29(2), 1-17.
- Bickerton, C. J. (2012). *European integration: From nation-states to member states*. Oxford University Press.
- Buchanan, A. (2004). *Justice, legitimacy, and self-determination: Moral foundations for international law*. Oxford University Press.
- Castells, M. (2009). *Communication power*. Oxford University Press.
- CNIL. (2019). Sanction de 50 millions d'euros à l'encontre de Google LLC. <https://www.cnil.fr/fr/sanction-de-50-millions-deuros-lencontre-de-google-llc>
- Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, 51(1), 133-204.
- Conseil constitutionnel. (2018). Decision no. 2018-765 DC of 12 June 2018. <https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm>
- E-Estonia. (2024). X-Road: Interoperability services. <https://e-estonia.com/solutions/interoperability-services/x-road/>
- European Data Protection Board. (2019, January 21). The CNIL's restricted committee imposes a financial penalty of 50 million euros against Google LLC. https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

- European Parliament and Council. (2016). Regulation (EU) 2016/679 of April 27 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*.
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 of June 13 2024 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*.
- Foucault, M. (1986). Of other spaces. *Diacritics*, 16(1), 22-27.
- Gill, G. (2003). *The nature and development of the modern state*. Palgrave Macmillan.
- Hegel, G. W. F. (1991). *Elements of the philosophy of right*. Cambridge University Press.
- Held, D., & McGrew, A. (Eds.). (2003). *The global transformations reader: An introduction to the globalization debate* (2nd ed.). Polity Press.
- Hobbes, T. (1996). *Leviathan*. Cambridge University Press.
- Islamic Consultative Assembly Research Center. (2023). Policy statement on promoting artificial intelligence governance. <https://rc.majlis.ir/fa/news/show/1778682> [In Persian]
- Jackson, R. H. (2007). *Sovereignty: Evolution of an idea*. Polity Press.
- Kalmo, H., & Skinner, Q. (Eds.). (2010). *Sovereignty in fragments: The past, present, and future of a contested concept*. Cambridge University Press.
- Kant, I. (2006). *Toward perpetual peace and other writings on politics, peace, and history*. Yale University Press.
- Kuner, C. (2017). *Transborder data flows and data privacy law*. Oxford University Press.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.
- Lefebvre, H. (1991). *The production of space*. Blackwell.
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Loi no. 2020-1266. (2020, October 19). Loi visant a encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne. *Journal officiel de la Republique francaise*.
- Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, 25(2), 185-213. <https://doi.org/10.1017/S0003975600004239>
- Mann, M. (2012). *The sources of social power: Vol. 1. A history of power from the beginning to AD 1760* (2nd ed.). Cambridge University Press.
- Morris, C. W. (2002). *An essay on the modern state*. Cambridge University Press.

- Nelson, B. R. (2006). *The making of the modern state: A theoretical evolution*. Palgrave Macmillan.
- Peers, S., & Ward, A. (Eds.). (2004). *The EU charter of fundamental rights*. Hart Publishing.
- Rousseau, J.-J. (2002). *The social contract*. Penguin.
- Salmani, Z., Sharifi, A., & Farkish, H. (2024). A study of the challenges facing citizens' rights in the Iranian administrative system based on good governance indicators. *Public Law Studies Quarterly*, 54(3), 1409-1433. <https://doi.org/10.22059/jplsq.2023.361460.3343> [In Persian]
- Schmitt, C. (2005). *Political theology*. University of Chicago Press.
- Shafiei Alavija, M., Mirhosseini, S. M., & Emadzadeh, M. K. (2025). An analysis of the challenges in protecting citizens' rights in Iran: A case study of the judiciary institution. *Public Law Studies Quarterly*, 55(1), 539-566. <https://doi.org/10.22059/jplsq.2023.355818.3274> [In Persian]
- Skinner, Q. (2014). *The foundations of modern political thought: Vol. 1. The Renaissance* (K. Firouzmand, Trans.). Agah Publishing. [In Persian]
- Walker, N. (Ed.). (2003). *Sovereignty in transition*. Hart Publishing.
- Weber, M. (1978). *Economy and society*. University of California Press.
- Yeung, K. (2018). *Algorithmic regulation*. *Regulation & Governance*, 12(4), 505-523.
- Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs.