Data & Policy (2026), 8: e44
doi:10.1017/dap.2026.10089

RESEARCH ARTICLE

Advancing data agency: A conceptual framework to support data sovereignty

Jaime Bernal

Copernicus Institute of Sustainable Development, Utrecht University, Netherlands
Email: jaimebernal743@gmail.com

Received: 19 June 2025 UTC; **Revised:** 30 June 2026 UTC; **Accepted:** 05 July 2026 UTC

Keywords: artificial intelligence; data agency; data sovereignty; data transfers; European Union

Abstract

The term *data sovereignty*—the principle that data is subject to the laws and governance of the country where it is collected or stored—faces implementation challenges. The legal deadlock over how to regulate transatlantic (E.U.–U.S.) data transfers reveal the difficulties of asserting "sovereignty" over data, a resource that flows transnationally through digital technologies. Among global regulatory efforts, the European Union's struggle to ensure the supremacy of its data protection and privacy laws represents an interesting case from which to derive new theoretical and conceptual insights. This paper advances *data agency*—as agency mediated *by* data, not *over* it. The intention is to advance a term that moves beyond the limits of data sovereignty to explain how governance over data-driven systems is distributed and contested. The manuscript suggests pragmatic pathways for more effective governance as mere "control" over data is not enough to achieve meaningful insights derived from data technologies.

Policy Significance Statement

The concept of *data sovereignty* has reached a discursive impasse, often inadequately explaining some regulatory policies given the complexities of global data flows and power asymmetries in the digital age. While the idea of "sovereignty" provides a crucial legal foundation for data governance, its overemphasis on control and jurisdiction often obscures more pragmatic pathways to benefit from data technologies. This paper argues for a necessary conceptual expansion towards *data agency*, a framework rooted in relational and distributed understandings of shared capabilities for decision-making and action. This framing can capture past E.U. policy decisions focused not on data localization, but on strategically building functional capacity, exporting its normative ideas and laws to other countries, and redistributing agency in the data economy through legal frameworks that promote more trusted data sharing, decentralized technologies, and democratic discussions.

1. Introduction

The capacity of individuals and groups to reflect on their routines and act according to their best interests—an exercise of agency—is increasingly mediated by data-driven technologies designed by actors whose goals do not always align with those of the users they serve. Information derived from such technologies does not merely inform decision-making and behaviour; it reconfigures the very structures that make these possible. For example, the spread and pervasiveness of algorithms on social media do not merely present content; they restructure how users allocate attention, form opinions, and perceive the world,

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

unprecedentedly altering the structure that organizes agency during human–machine interactions. This paper advances a conceptual framework for the study of the interplay between data and agency. In its broadest sense, *data agency* is not merely agency *over* data, but agency *mediated by* data.

This construct is intended to empower widespread political and academic discourses that call for greater sovereignty over data at the individual, organizational, or national levels. Nonetheless, this requires to also reflect and critiquing these discourses for failing to account for how control over information flowing from digital technologies is distributed and contested. Only in this way can advocates for structural change in the governance of data arrive at a compromise between control and meaningful use.

Recognizing the growing societal effects of data technologies, the European Commission, through its *European strategy for data*, sought to articulate a vision for the European Union to "become a leading role model for a society empowered by data", justifying the imperative of increasing the access, sharing and use of data among more societal actors and sectors (European Commission, 2020a, p. 1). To support this agenda, the term "sovereignty" became a word choice in policy and academic discourses (Adler-Nissen & Eggeling, 2024; Pohle and Thiel, 2020). Over the years, the concept of *data sovereignty* gained popularity amidst political and legal scandals (e.g., the 2013 Snowden revelations, the rulings of the *Max Schrems I* and *II* cases, or the 2018 Facebook–Cambridge Analytica affair). Nonetheless, in an interconnected world and digital space, national policies worldwide designed to increase control and decrease external reach have proven to be difficult to implement and, in some cases, undesirable for economic growth and global governance (Chander and Sun, 2023). Such tension is set to continue to be a matter of discussion among key internal members and external partners in every digitalized country.

In the E.U. context, proposed policies to increase sovereignty in the cloud have failed to reach agreement in the past (DIGITALEUROPE, 2022; Chee, 2024). Nevertheless, in 2026, the European Commission launched the Tech Sovereignty Package, introducing a relatively more open-ended framework for interpreting sovereignty-oriented requirements for certain sensitive data processed in the cloud than past proposed regulations. Notably, the communication of the strategy includes guidelines to promote technological independence through open-source software development (European Commission, 2026).

Amidst increasing warfare, geopolitical and geoeconomic tensions, and systemic changes in global trading and financing due to the crisis of the liberal order marked by U.S. hegemony, there is stronger recognition that building the necessary infrastructure to host domestic data in order to shield the most sensitive types while promoting technological self-reliance through open-source software is strategically vital. As such, this manuscript calls for a reflection on previous policy decisions to provide lessons for the future and to balance the tensions between global data flows and the protection of domestic data.

By introducing data agency, this manuscript argues that certain framings provided by the idea of sovereignty should be rethought and, in certain respects, abandoned. Making room for new terminology is necessary so policymakers can better articulate how the growing influence of data technologies is shaping human lives and the world's dynamics amidst pervasive surveillance, expanding asymmetries—where fewer entities increasingly control larger volumes of data—and the rise of machine–human interaction, which simultaneously empowers and diminishes human agency.

Following this introduction, the paper provides a critique of "data sovereignty," reflecting on its deviation from its original understanding as the principle whereby the use of data is subject to the laws of the country where it is stored or processed (Irion, 2012). While widely invoked in policy and academic discourse, data sovereignty has become too ambiguous and overextended. It spans multiple domains—from cross-border legislation and IT infrastructure to healthcare—and applies to diverse actors, from states and organizations to citizens and Indigenous communities (Hummel et al., 2021). Sovereignty covers a whole range of heterogeneous notions depicting legal control, ownership, privacy, national security, and inclusion, making it difficult to operationalize. Nonetheless, sovereignty remains a powerful concept for claiming one's rights but, which, nevertheless, can also transform the term into what philosophers and linguistics warned: an empty signifier (i.e., a concept that has become obsolete due to its overuse) that fails to promote its intention of emancipation.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Section 2 analyses the unresolved dispute between the European Union and the United States over transatlantic data transfers and the commercialization of the term data sovereignty as a cloud solution as an illustrative case that highlights Europe's difficulties in guaranteeing the supremacy of local laws over foreign ones. Section 3 advances the concept of data agency, exploring the philosophical foundations of relational and distributed agency and its interplay with data, analysing how (data) structures shape (data) agency and vice versa, as well as how increasing human–machine collaboration reconfigures exercising agency. Building on this conceptualization, Section 4 discusses how data technologies are reshaping global economies and outlines forward-looking recommendations for mitigating the potential downsides and exploiting the advantages of a world where agency is ever more channelled by data technologies, including regarding data transfers.

2. Critique of data sovereignty

Polatin-Reuben and Wright (2014, p. 1) define data sovereignty as a "catch-all term" that, nonetheless, includes "the attempt by nation-states to subject data flows to national jurisdictions." Yet, the use of this concept has extended significantly across several symbolic networks, as shown in Hummel et al.'s (2021) review of 341 publications, which finds wide disagreement about which agents (e.g., individuals, organizations, states) sovereignty applies to, what values it denotes (such as control, privacy, and ownership, inclusion), and in which contexts.

First, data sovereignty has been evoked in various domains concerning cross-border data flows legislation (e.g., debates about data localization), IT infrastructure (e.g., European cloud projects), medical research (e.g., patient data rights), and societal affairs (e.g., Indigenous peoples' data governance). Second, data sovereignty can be attributed to diverse agents, including states asserting authority over national data infrastructures, organizations managing access to proprietary datasets, individual citizens seeking control over personal data, and Indigenous communities claiming governance over data concerning their peoples. Third, data sovereignty can be understood in multiple ways: as an ability or capacity (e.g., to determine the conditions of data access), a right (as in data-subject rights under privacy law), the outcome of specific legislation (such as data governance frameworks), a means of enabling beneficial data use (through controlled sharing), or a matter of confidentiality and national security (e.g., limiting foreign access to sensitive datasets), and even an extension of traditional sovereignty claims into the realm of data technologies. Finally, the values that underpin data sovereignty are also heterogeneous, including principles such as control, power, and ownership (over data use and infrastructures), the protection of privacy and the regulation of data flows, and broader normative ideals such as inclusive deliberation, representation, and participation in data governance (Hummel et al., 2021).

The historical resonance and global relevance of "sovereignty" make it a powerful root word, often paired with prefixes specifying the domain or resource asserted—such as health or food. In this sense, sovereignty functions as a *master signifier* in societal discourse, its popularity stemming from its ability to symbolize and structure a broad network of meanings within ideological discourse (Laclau and Mouffe, 1985). To preserve their appeal, signifiers like "sovereignty" (e.g., democracy, communism, and justice) should remain ambiguous and open to diverse interpretations, serving as nodal points around which other signifiers stabilize, regardless of disparity. For example, energy sovereignty might encompass various environmental, economic, political, and social dimensions. The paradox is that this success comes at a cost—the more the signifier tries to unify different elements, the more it risks emptying itself of determinate meaning.

Different actors—governments, corporations, activists, and citizens—continue to struggle to define what sovereignty over data means. Thus, its meaning is highly contingent, shifting over time depending on the balance of power, technological advancements, and ideological movements. This flexibility may render signifiers like sovereignty "empty signifiers" which "name the positive reverse of an experience of historical limitation" (Butler et al., 2000, p. 185). Indeed, data sovereignty is evoked in a particular historical setting by communities who precisely lack control over data. Because fulfilling the goal of having *absolute* control over data flows is seemingly unfeasible (Polatin-Reuben and Wright, 2014), empty signifiers like data sovereignty emerge to represent the absence of such completeness.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

There is broad consensus that data, as a strategic resource, is increasingly the object of competition between sovereign states striving to control its flow while balancing national interests. Yet globalization and the Internet have eroded "the ability of states to control movement across their borders," including information (Krasner, 2001, p. 19). The multidimensional architecture of digital information functions as a "rhizomatic" system of non-hierarchical, interconnected nodes that blur lines between virtual and real, transcend boundaries, elude state control, bypass consent, and challenge cybersecurity protocols (Mueller, 2020). Substantial gaps in controlling data flows may always exist. Still, laws to manage digital information across borders will continue to emerge.

Although sovereignty is often invoked to pursue specific ends, such as autonomy, wealth or security, it tautologically refers to itself only—it can be demanded for its own sake, as its self-referential semantics show (Přibáň, 2015). Sovereignty retains significance simply because it asserts its own importance, which perpetuates its relevance in the discourse. Ultimately, the reliance on the term "sovereignty" to claim control over data has allowed for the construction of a more coherent and persuasive narrative. Inadvertently, nowadays, its success as a discursive frame is limiting a more holistic view that focuses on other aspects of the data value chain such as how data generates value for different actors, how infrastructures are designed and organized, how power and benefits are distributed across the ecosystem, or how dependencies constrain effective participation.

Seeking a binary legal understanding of data sovereignty (i.e., whether a country's data laws prevail over others) may be counterproductive. Concepts like the supremacy of law and its extraterritoriality are neither absolute nor guaranteed but shaped by real-world factors such as states' and organizations' capabilities and actions to control data. Data sovereignty is thus better linked to an evolved understanding of sovereignty as the pursuit of governmental action, rather than the Westphalian idea of absolute state authority over territory. This renders sovereignty an empirical issue, characterized by nuance (March and Scieferdecker, 2023). Therefore, a more productive analysis of data sovereignty would shift the question from *if* a state is sovereign to *how* it is sovereign, asking: To what extent, and through what specific actions and capacities, can a polity like the E.U. govern data flows within and across its borders? Consequently, the broad, forward-looking interpretation of "sovereignty" in the digital realm—as "a community's empowerment and its ability to control its destiny" (Rikap et al., 2024)—aligns not with a static claim of control over data, but with the dynamic, capacity-oriented concept of data agency.

The remainder of this section explores the challenges faced by the European Union in the context of transatlantic data transfers as a case study to understand how some E.U. policy decisions did not just pursue data sovereignty but also cultivated data agency. The issues surrounding the regulation of global data transfers offer an illustrative case of the conceptual limitations of data sovereignty and the need to develop new terms.

2.1. Transatlantic data transfers

The E.U.–U.S. cross-border data relationship is the largest one and underpins $7.1 trillion in trade and investment (The White House, 2022). However, this relationship is highly asymmetrical. Despite Europe's larger population size and economic output, the European Commission (2021, p. 3) estimated that 90% of the European Union's data is managed by U.S. firms. Such an imbalance has created difficulties for enforcing the European Union's relatively stronger privacy and data protection standards (while also influencing the evolution of these standards over the years) (Farrell and Newman, 2016).

Before the 2013 Snowden leaks, Irion (2012) warned that cloud computing posed legal risks by exposing public data to foreign laws and third-party access. This issue gained prominence after the exposure of the U.S. National Security Agency's (NSA) upstream and downstream surveillance practices (Lyon, 2014). The former involved collecting communications as they traversed the Internet backbone, and the latter, exemplified by the PRISM program, facilitated intercepting electronic communications and data from major tech companies like Google, Microsoft, Facebook, and Apple. For example, upstream surveillance allowed agencies to tap into phone communications, while downstream surveillance enabled the collection and analysis of electronic signals gathered by devices, also known as signals intelligence

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

(SIGINT). Following the global outcry triggered by the leaks, the challenge of exerting authority over data was highlighted (De Hert and Boulet, 2013).

During the post-Snowden decade, the European Union has proposed, negotiated, and implemented several regulations governing the flow of data to the U.S. The General Data Protection Regulation (GDPR) is the most consequential, as it regulates transfers of personal data outside the European Union (European Commission, 2016). Meanwhile, provisions in the Data Governance Act (European Commission, 2022) and the Data Act (European Commission, 2023a) were designed to prevent unlawful transfers as well as governmental third-party access. However, while E.U. regulators have aimed to shield local data from third-party access, the U.S. government has approved laws that allow its agencies to tap into data produced abroad, whether stored locally or overseas.

Among others, Section 702 of the 1978 U.S. Foreign Intelligence Surveillance Act (FISA) allows surveillance of foreign entities and individuals. Targets extend beyond terrorists and criminals to include foreign officials, diplomats, journalists, and others whose communications are deemed to hold intelligence significance (United States, 1978). Similarly, the 1981 Executive Order (EO) 12,333 on SIGINT gives the authority to gather, retain, analyse and share foreign SIGINT (Department of Defense, 1981). The 2001 USA Patriot Act grants broad surveillance powers for counterterrorism (United States, 2001). Finally, the 2018 CLOUD Act gives authorities the right to request from service providers data stored abroad (Department of Justice, 2018).

Despite the fact that government access to data for national security purposes falls under Member State competence pursuant to Article 4(2) of the Treaty on the European Union (European Union, 1992/2007), which reserves national security as "the sole responsibility of each Member State," the tension remains: the European Union's data protection framework is in contradiction with U.S. law. Furthermore, around two-thirds of the cloud market is controlled by a handful of U.S. firms (Synergy Group, 2020). Hence, making it complex for native cloud providers to scale within the E.U. territory.

Due to the extraterritorial components of the European Union's privacy and data protection laws, the region faces difficulties enforcing these rules in the context of transatlantic cross-border data transfers. Under Article 45 of the GDPR, the European Commission can issue "adequacy decisions"—determinations that a non-E.U. country provides a level of personal data protection essentially equivalent to that guaranteed within the European Union (European Commission, 2016). Such decisions enable the free flow of personal data to that foreign country without requiring additional safeguards. However, the Court of Justice of the European Union (CJEU) has twice invalidated the Commission's adequacy decisions in the context of E.U.–U.S. data transfer frameworks—Safe Harbor in 2015 (Schrems I) and Privacy Shield in 2020 (Schrems II)—ruling that the United States. failed to provide adequate protection of personal data (Tracol, 2020).

The 2016 Privacy Shield, which over 5300 businesses depended on, was ruled invalid by the CJEU in the Schrems II decision. The Court ruled that U.S. law permitted excessive bulk data collection without adequate safeguards and failed to provide E.U. citizens with an effective judicial redress mechanism, falling short of the "essentially equivalent" protection required by the GDPR (Tracol, 2020). In response, the 2023 Data Privacy Framework sought to address these deficiencies. It introduced the principles of "necessity" and "proportionality" to limit bulk data collection and established a two-tier redress mechanism: a Civil Liberties Protection Officer (CLPO) for initial complaints, with a second-tier review by a newly created Data Protection Review Court (DPRC) composed of members independent from U.S. intelligence agencies (European Commission, 2023b).

However, between the invalidation of the Privacy Shield in 2020 following the Schrems II decision and the implementation of the 2023 Data Privacy Framework, E.U.–U.S. personal data transfers remained legally uncertain. While transfers could continue using alternative mechanisms such as standard contractual clauses (SCCs), these contractual safeguards do not bind third parties, including government authorities, and thus cannot address the fundamental concern of U.S. intelligence access to E.U. data.

Following a binding decision by the European Data Protection Board (EDPB), the Irish data protection authority issued a landmark €1.2 billion fine to Meta Ireland in May 2023, coinciding with the GDPR's 5th anniversary (European Data Protection Board, 2023). More specifically, Meta failed to protect

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

E.U. data subjects against U.S. Section 702 of FISA. The core of the finding was that Meta's chosen legal mechanism for transfer (SCCs) was invalidated because it could not protect the data in practice from access by U.S. public authorities under laws like Section 702 of FISA.

In its first periodic review of the Data Privacy Framework, the European Commission offered a positive assessment of the framework (European Commission, 2024a). Soon after, the EDPB applauded the progress but criticized the lack of proactive compliance checks by the U.S. Department of Commerce (DoC) and the Federal Trade Commission (FTC), arguing that the low number of complaints does not necessarily indicate compliance (European Data Protection Board, 2024). Furthermore, the controversial Section 702 of the 1978 U.S. FISA, set to expire in late 2023, received a temporary extension until April 2024, followed by a 2-year extension, making it a topic of debate until the next decision in 2026 (Marquis, 2024). Legally, there is an uphill struggle ahead in defining the future of the largest and possibly most asymmetrical (in absolute terms) data relationship in the world. Given that a resolution to this legal struggle appears unlikely in the foreseeable future, an analysis focused solely on the pursuit of the idea of data sovereignty in the strictest sense may fail to capture the less ambitious but more pragmatic tactics currently being discussed in the E.U. regarding the exploitation of data technologies and use.

2.2. The commercialization of data sovereignty

As E.U. data producers, from organizations to individual, lack strict sovereignty over their data in the context of transatlantic data transfers, and despite legal efforts to address this issue, the idea of "data sovereignty" gradually took on a new meaning: as a commercialized solution based on data localization. This can be exemplified by the European Union Agency for Cybersecurity's (ENISA) Cybersecurity Certification Scheme for Cloud Services (EUCS) draft, which proposed "sovereignty requirements" mandating that for certain categories of data held by critical entities such as government bodies, healthcare services, and critical infrastructure providers. Under the EUCS, cloud service providers (CSPs) must ensure that data processing and storage occur exclusively within the European Union to safeguard sensitive data from non-E.U. jurisdictions (European Union Agency for Cybersecurity, 2020). The draft also specified that CSPs seeking to achieve the highest security assurance levels would need to maintain their global headquarters and key operational offices within the European Union, which would potentially exclude foreign CSPs.

The *hyperscalers*—Amazon (AWS) (Amazon Web Services 2022, Microsoft (Azure) (Microsoft, 2022), and Google (Google Cloud, 2022)—announced data sovereignty solutions to ensure "cloud on Europe's terms." These offerings promised to keep data within European borders and employ local staff to oversee operations but did not address the fundamental issue of foreign government access. This is due to the scope of U.S. laws, such as FISA or the CLOUD Act, which allow U.S. public authorities to access data stored abroad. Meanwhile, some European CSPs, immune to foreign law, positioned themselves as aligned with the European Union's data sovereignty agenda (OVH, 2022). Yet, as latecomers into the industry, they face limitations in developing the competitive products offered by the American scaling giants, particularly for training cutting-edge AI systems that require extensive computational power (Bauer and Lamprecht, 2023; Blancato, 2024). As a result, the term "data sovereignty" was appropriated by both local and foreign CSPs.

Industry groups warned that Europe should not exclude foreign CSPs offering the latest technologies, as this could harm the local ecosystem (Chee, 2024). Although the sovereignty requirements targeted data controlled by critical entities, lobbyists argued this could lead to broader restrictions. Restricting access to foreign CSPs was viewed as counterproductive, as local companies could not match the advanced technologies and prices of established providers (DIGITALEUROPE, 2022; Bauer, 2023). Additionally, claims were made that the sovereignty requirements violated World Trade Organization principles (Center for Strategic and International Studies, 2023). The recurring argument against sovereignty calls is that Europe risks excluding itself from economic growth and technological progress. Ultimately, the sovereignty requirements in the draft of the EUCS were discarded.

European cloud companies might not narrow the transatlantic data asymmetry in the short term (Blancato, 2024). Despite rising revenues, they are losing market share to their U.S. counterparts (Synergy

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Research Group, 2022). Because U.S. cloud giants continue to offer their latest services to European customers, the purely market-driven incentive to develop a robust native infrastructure is less apparent. However, this commercial reality exists in tension with strategic goals for competitiveness, sovereignty, and reduced external dependency. Simultaneously, the European Union cannot block foreign CSPs to increase the urgency to grow its own infrastructure, as U.S.-based CSPs offer scalable, cutting-edge solutions upon which ancillary critical technologies depend.

The transatlantic data relationship can be understood through the lens of the North–South dependency theory of economic development. Between the United States and the European Union, one observes key "features of the periphery and semi-periphery relations" such as "a high penetration by foreign capital" and "a heavy technological dependence" (Tausch, 2010, p. 469). Nonetheless, as the new interdependence approach highlights, overlaps also create power asymmetries that offer new opportunities to non-state actors (Farrell and Newman, 2016). In this regard, one can observe how new players, from transnational businesses to privacy activists (e.g., Max Schrems), are playing a crucial role in defining the future of transnational data transfers.

2.3. Beyond sovereignty

The previous subsections have highlighted three limitations of data sovereignty as an analytical concept. First, the term is highly contested and unstable, encompassing diverse actors, objectives, and governance arrangements. Second, because exercising control over data flows is challenging due to the technical architecture of the Internet and the realities of global interdependence, makes data sovereignty an effort that either demands: (1) greater cooperation with countries that export data originating in the European Union to reconcile legal frameworks between worldwide jurisdictions, or (2) the development of E.U.-based autonomous technological, legal, and infrastructural capacities capable of reducing external dependencies. Both efforts should be pursued. Third, the discourse of data sovereignty has increasingly been translated into commercial and infrastructural solutions—particularly cloud localization strategies that do not necessarily resolve the underlying challenges of foreign laws, technological dependence, or asymmetric market power.

To explain why E.U. policy is struggling to resolve the mismatch between its strong data protection and privacy laws and the United States's comparatively weaker laws regarding access to foreign data, one could focus on the institutional, political, and economic constraints that shape policymaking in an interdependent digital economy. Such an analysis would not only pay attention to the struggle to coordinate and implement a successful strategy among E.U. internal stakeholders or to the expensive lobby efforts from domestic and foreign firms that have strongly shaped policy decisions during the first quarter of the 21st century, but also to a long-lasting mutual interest in maintaining high cooperation between the European Union and the United States over security and diplomatic issues (Farrell and Newman, 2019). Indeed, taking a drastic legal shift to force the supremacy of local laws over U.S. law might not have been in the best strategic interests for most of the E.U. Member States, at least, for now.

Contributing factors to this deadlock include an incapacity to defuse key U.S. chokepoints in the digital economy (i.e., structural leverage the U.S. wields through dominant tech platforms and critical financial and technical infrastructure) (Farrell and Newman, 2023), potential cybersecurity risks regarding data localization mandates (Swire et al., 2024), and fears of retaliation and missing out on the latest cloud offerings (Bauer and Lamprecht, 2023). This complex web of constraints illustrates some of the practical limits of data sovereignty as a concept in the face of geopolitical and economic realities. It shows that the ultimate policy goal is not just to create a sense of sovereignty and independence in the Union. Sovereignty, to yield benefits to the European Union and beyond, needs to be complemented by innovative governance to avoid the catastrophic consequences of deglobalization and the weakening of multilateralism (despite all its flaws).

The E.U.–U.S. data transfer negotiations have been presented by American think tanks as an impossible "trilemma" for E.U. lawmakers, who were said to need to prioritize only two out of three conflicting realities: (i) the protection of citizens' right to privacy, (ii) unrestricted data flows, and

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

(iii) personal data collection by U.S. intelligence agencies (Barker, 2020). Whether this trilemma will continue to restrain the European Union's policy decisions will depend on its efforts to build the necessary infrastructure to match the capabilities of United States and find new partners overseas.

Conversely, an alternative, pragmatic analysis would focus on what the European Union has achieved by delaying full alignment with either approach: unrestricted data flows or strict data localization. Rather than interpreting regulatory fragmentation as policy failure, it can be understood as a form of strategic positioning to preserve regulatory power across more domains. Regarding data technologies, the European Union has succeeded in exporting its standards worldwide, influencing other jurisdictions. It has, arguably, benefited financially from investment inflows and knowledge-sharing (e.g., the concentration of data centres in the Netherlands and Ireland), and from access to frontier AI and cloud technologies, while also shaping the terms under which these technologies are deployed in the world's markets. In addition, the European Union has increased bargaining power in transatlantic negotiations by repeatedly forcing the renegotiation of adequacy frameworks. These dynamics illustrate that the struggle to pursue sovereignty has generated other forms of indirect influence that extend beyond territorial control of data infrastructures.

Furthermore, the European Union has also envisioned how policy can stimulate the data economy, as reflected in the following policies. First, building federated cloud infrastructure by funding projects like the Gaia-X initiative to create an interoperable cloud ecosystem. Unlike a single "EU cloud," Gaia-X is designed as a standards-based network that allows different cloud providers to connect, enabling data and service portability, and reducing dependency on any single vendor (Gaia-X, 2024). Second, establishing a legal framework and funding data intermediaries through Chapter III of the Data Governance Act, the European Union is fostering new business models for secure data sharing (European Commission, 2022). Third, empowering users with rights: The right to data portability in the GDPR allows users to obtain and reuse their personal data across different services, making it easier to switch providers and thus reducing barriers to competition (European Commission, 2016). Opinions on the GDPR's effects vary; some argue that the regulation concentrates market power and limits data-driven innovation by restricting data sharing (Gal and Aviv, 2020), while others claim that user rights can encourage compliance-driven and incremental innovation (Blind et al., 2022). Fourth, preventing vendor lock-in: Chapter IV of the Data Act mandates that cloud providers allow customers to switch to rival services without prohibitive costs or technical obstacles (European Commission, 2023a).

Key to understanding this vision is the fact that the abovementioned efforts in the European Union have been complemented by discussions around implementing privacy-enhancing techniques (PETs) (Farrell et al., 2023; Hurtado Ramírez et al., 2023) and advancing open-source software infrastructure (European Commission, 2020b). PETs comprise technologies that allow data to be analysed for insights without being centrally gathered or directly exposed. The European Commission's strategy positions open-source development as central to technological sovereignty, minimizing lock-ins and reducing dependency on non-E.U. tech giants.

From this perspective, what emerges is not a lack of sovereignty, but rather a partial and evolving form of influence exercised through regulatory, legal, and market-based instruments. This is where the concept of data agency becomes useful. Data agency shifts attention away from whether actors possess absolute control over data and, instead, focuses on the capacities through which they can shape data flows, structure incentives, and impose norms within interdependent systems. In the E.U.–U.S. context, this includes the ability to set extraterritorial compliance standards, to leverage Europe's large market size to export regulatory norms, and to mobilize institutions to recalibrate transatlantic data governance. This is more than sovereignty.

3. Data agency

The concept of data agency should not be reduced to agency over data. This interpretation overlaps with existing notions related to sovereignty and power, while overlooking key dimensions of data-mediated agency unrelated to control and/or jurisdiction over data (sovereignty) (Hummel et al., 2021; Hellmeier

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

and von Scherenberg, 2023) or influence and dominance of others through it (power) (Beer, 2009; Couldry and Powell, 2014).

Baconian agency is marked by a recursive relationship between knowledge and power, where the discovery of causes (through knowledge) that produce certain effects enables the ability to direct them (through power) (Enfield and Kockelman, 2017). In this sense, data agency shares similarities with data power (both could interpret data technologies as tools to exercise control), but they differ in important ways. Data power is understood as power over others through information derived from data or algorithmic decisions (Lynskey, 2019). Even though data agency can pre-empt data power, it does not necessarily involve dominating others or processing their data without individuals' consent (Andrejevic, 2014).

Indeed, agency is interwoven among structures of power and knowledge and, despite being constrained by these external forces, resistance as agency is possible (Foucault, 1978). Crucially, this means data agency can be exercised without subordinating others. Consider, for instance, individuals using personal informatics tools that enable selective disclosure. Through these tools, users can cultivate data agency by generating, interpreting, and acting on information to guide decisions about sleep, medication, or exercise, for example (Li et al., 2010). This type of agency could become more and more decentralized, arising from oscillating interactions between users and the data they produce. It strengthens evidence-based self-understanding and adaptive decision-making without subordinating others or relying on anyone else's data without their consent.

Having agency means the capacity to identify and engage with what is intelligible (Negarestani, 2018)—in other words, "making sense of the world so as to act within it" (Couldry, 2014, p. 891). The instrumental agency available in the age of data technologies is both a means and an end: a means to achieve societal goals (e.g., better health outcomes or economic efficiency) and an end in itself as a form of cultivated potential (e.g., data literacy, analytical infrastructure, and actionability). In other words, it is a tool that individuals, organizations, and states use to enhance their agency (Enfield and Kockelman, 2017). Building this capacity becomes a primary strategic objective for empowerment in a data-driven world. Thus, works on digital agency focus on education (Siddiq et al., 2024; Vartiainen et al., 2024), and the sociological idea of agency as "the capacity of human beings to shape circumstances in which they live" (Emirbayer and Mische, 1998, p. 965).

Hence, data agency could be conceived as a form of meta-agency—the capacity to reflect on and influence one's own agency to act in the world. It goes beyond the reactive, ex-post reflexivity of data-driven decision-making, which might involve following predefined metrics or algorithmic outputs. Data agency is a second-order capacity: it is an exercise in questioning metrics, understanding, shaping, and constructing algorithms for decision-making, and reconfiguring the very systems through which data informs action.

Moreover, agency exists across networks of human and non-human actors and is increasingly shaped by the new ontologies constructed by data technologies. This process deepens the levels of intelligibility by introducing qualitative (e.g., indices, classifications, and sentiment models) and quantitative (e.g., scores, metrics, and probabilities) dimensions to symbolize the world and manage global challenges, from climate adaptation to public health crises, and the protection of animals. As such, data agency encompasses the data-mediated, oscillating distribution of agency across human and non-human networks.

Once interpreted and operationalized within a technical or social system, data functions as a pivotal mediator of distributed agency (Enfield and Kockelman, 2017). In a relational sense, data acquires an agentive capacity by shaping the possibilities, interpretations, and actions of agents within a network (Latour, 1999). Thus, it is not the raw, uninterpreted data itself, but the socio-technical systems of interpretation and action that operationalize data in channelling agency.

The next sections explore how structures shape agency and how agency emerges from structures (Kennedy et al., 2015). "Structures" refer to the networks of human and non-human agents, including the technical specifications, components, and broader economic and socio-political frameworks that influence the data value chain. Agency is deeply embedded and distributed across such structures. Thus, data agency is not simply constrained by structures but actively reconfigures them. Crucially, data agency is

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

neither external to nor simply constrained by these systems; it is deeply embedded within them. This leads to a recursive relationship: the structures of a system shape the agency possible within it, and that agency, in turn, can reconfigure the structures themselves.

3.1. Structures in agency

Agency can be understood as a distributed capacity that emerges from interactions (Enfield and Kockelman, 2017). For example, consider the data agency involved in a near-miss encounter between an autonomous vehicle and a pedestrian guided by an online map. Agency in this situation is not located solely in the car's algorithm or the pedestrian's journey, but emerges from the dynamic, data-mediated interaction between them. This perspective shifts the focus from who has agency to how agency is constituted and exercised within a network.

Although agency mediated by data technologies differs from human agency, understanding the latter helps conceptualize the former. In the body, sensory stimuli (light, sound, touch, etc.) are transformed into neural signals (data that turns into information) and are subsequently interpreted by the brain to generate (un)meaningful perceptions of the external world. This enables individuals to understand and interact with their environment, forming the basis for human agency (Kant, 1785/2011). In this Kantian view, agency is tied to rational autonomy, a capacity to act based on principles that transcend external forces. For instance, an individual's capacity to demand transparency about their personal data is contingent on legal frameworks like the GDPR's "right to explanation" (European Commission, 2016).

While machines' *apparent* agency can be reduced to a set of processes (machines may emulate human agency by assembling computations to simulate thought and action (Wooldridge and Jennings, 1995), true agency is highly relational, shaped by the interplay of internal capabilities and external influences (Negarestani, 2018). This relational perspective provides the crucial link for understanding agency in a world where a lot of data could be relevant to tackle societal challenges but often remains untapped and not curated (Susha et al., 2022).

In socio-technical systems, internal capabilities to cultivate data agency include human cognition (e.g., domain expertise, interpretive flexibility, data literacy, and critical judgement), but also computational power, algorithmic design, and adaptability of non-human systems—exemplified by multimodal systems that synthesize data from diverse sources (text, images, and sensors) into coherent, potentially interpretable data (Devlin et al., 2018). Key external influences for organizations and academics to focus on encompass social and legal norms, the technical architectures of data flows, the market dominance of platforms with large scaling power, and the geopolitical realities of digital infrastructures. Data agency, therefore, is the capacity that emerges from the continuous interplay between these human and non-human agency-mediating agents. If collaboration is pursued across the data value chain, nations, regions, and the world can better serve citizens and achieve adaptive resilience to crises.

Thus, data agency is a dynamic and relational process channelled by internal and external human and non-human structures. Agency, rather than being independent, is distributed and oscillating. It is not solely under the sovereignty of the rational subject as understood by classical philosophers. Neither should it be under the control of governments, or other organizations, such as institutions or businesses.

3.2. Agency in structures

Collected data can be a tool of *self-relation* to render the world intelligible and guide actions. In the Hegelian sense, self-relation refers to the process by which *Geist* (spirit) understands itself through reflecting on its own development. As Negarestani (2018, p. 26) puts it, "Geist utilizes the intelligibility of its structural transformations (its history) as a model for conceiving itself." In the realm of data agency, self-relation involves how individuals, organizations, nations, and the international community use data to understand causes and effects, inform their decisions and actions, and evaluate the resulting outcomes. Information obtained from data is a necessary tool for self-reflecting and discerning patterns in one's history and, accordingly, guiding the evolution of Geist.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Latour's (1999) actor–network theory emphasizes that agency extends to non-human entities. Actor–networks are made of human and non-human actants, including inanimate, immaterial, and abstract entities, such as technologies, organizations, and ideas. As actants interact, they produce actions and reactions in one another. Data channels agency across networks of actants. Thus, agency is distributed within and across these networks, rather than contained within individual actants. Data agency is a collective endeavour; it exists in the relations between actants that process, interpret, and act based on data. Thus, the concept of data agency is a relational process with internal human and non-human characteristics and is influenced by internal individual bodily processes, ideology, technological parameters, social structures, and the ever-changing nature of the world.

Agency, in this context, is the ability to act based on this understanding, and the concept of data agency may articulate how this capacity is increasingly mediated by data technologies. Thus, data agency can be seen as an iterative process where data are used to understand the past and shape the future. The cyclical nature of self-relation is crucial for continuous improvement and adaptation. Therefore, data-driven self-relation requires awareness of transformative eventualities that redefine paradigms. In confronting global crises, for instance, cultivating agency requires a commitment to disruptive truths that expose systemic risks over comforting models. This aligns with Badiou's (2006) philosophy of the "event"—a radical rupture that reconfigures the state of affairs and his idea of "fidelity," which refers to the courage to acknowledge the truth of events that reshape the world, no matter how uncomforting.

3.3. The agency paradox of human–machine collaboration

Data technologies are reshaping individuals, organizations, institutions, and economic, political, and social relations, and so forth to create a new mode of production based on an "organising inorganic" digital regime that is reshaping agency in unprecedented ways (Hui, 2019). The "organising" encompasses, among others, the effects of data technologies in the world, while the inorganic refers to the fact that these objects are not organic like animals, plants, or fungi. This regime is shaping the myriads of forms of how humanity could develop. In the context of human–machine collaboration, questions about intentionality, motivation, self-efficacy, and self-regulation ought to be thoroughly examined to cultivate agency (Sharma et al., 2024).

This challenge is fuelled by the libidinal systematic transformation of individuals' sense of privacy, cognitive abilities, addictive behaviour, dependencies on technology for everyday life, social behaviour, and creativity. Users' interactions with data technologies create the raw material to train algorithms and, sometimes, arguably, not in their best interest or the common good. While the constant processing of data does not always align with the aforementioned elements, it has the potential to train systems' capacity to digest complexification by anticipating and increasing actionable control over future eventualities. Paradoxically, the very effects of data technologies in the world increase this complexification, nonetheless.

When high data quality is pursued, and biases are minimized, and when the currently controversial high centralization of data's capacity to function as an effective "means of prediction" is increasingly decentralized and democratized (i.e., not under the control of a few platforms, organizations, or governments), data agency can be better cultivated. Therefore, shifting to governance modes where individuals have greater sovereignty and agency over data, a more sustainable and fairer world can be pursued (Kasy, 2025).

For Kant, agency includes the capacity to reflect on one's actions through reason and shared principles. Yet intricate computational mechanisms in data technologies can resist human understanding (black-box reasoning). Here, accountability is rendered opaque, such as in self-driving car accidents, unclear healthcare diagnostics, or mistaken predictive policing. Nevertheless, such opacity is also present in the human brain and its theoretical Freudian unconscious, as information processing in both biological and algorithmic systems is distributed across multiple layers of processing, weakening the traceability between intention and action.

Yet, arguably, the most powerful and accurate AI models might operate beyond human understanding, whereas those designed to be transparent and accountable are often perceived as less capable

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

(Samek et al., 2021). The challenge is to balance machines' efficiency and complexity with human ethics (Saeed and Omlin, 2023). Critically, however, for example, large language models (LLMs) fundamentally lack the capacity for genuine critical thinking and creative problem-solving, as they operate through inductive probability over trained data arbitrarily chosen for a variety of goals (Johnson et al., 2022). Hence, AI systems should be designed to augment human capabilities by handling routine computational tasks while allowing individuals to retain authority over creative direction, strategic thinking, and normative judgement (Heer, 2019).

Still, a fundamental constraint is emerging: the stock of publicly available web data for training is finite and may be exhausted soon (Villalobos et al., 2024). This scarcity validates the industry axiom that for advanced AI, data quality often matters more than complex algorithms. Consequently, the strategic focus of European Union is shifting from pursuing "bigger" models to enabling access to "better" data (International Data Spaces Association, 2025). Unlocking this value requires solving a core challenge related to trust, as private actors are deeply reluctant to share sensitive operational data (Bernal, 2024).

The European Union has a dual strategy in this regard, which entails, first, fostering business-to-business and business-to-government data sharing through trusted, sovereign frameworks like data spaces; and second, pioneering technical architectures such as generator-verifier systems to allow businesses to confidentially train a model or verify outputs against their private data, enabling the model to provide answers without revealing the underlying proprietary information (International Data Spaces Association, 2025). This approach exemplifies the cultivation of data agency vis-à-vis data sovereignty: building the infrastructural and governance capacity to act on data (training powerful AI) without requiring entities to cede sovereign control over it.

AI tools can enhance user agency in some areas, but they may also diminish it by creating "cognitive lock-ins" that reshape mental processes for everyday tasks like recalling information, generating content, or solving the everyday challenges that organizations and individuals face (Hansen, 2024). The key question remains: In a world of pervasive data flows and rapid technological change, how can regulators cultivate meaningful agency through laws that govern the processing of data?

To make the most out of data technologies, the European Union must recognize and operationalize the relational and semiotic dimensions of humans as well. Neither machines nor humans alone can fully harness the complexity of societal systems. Yet, unlike machines, humans possess *semiotic agency*, or the capacity to engage in semiotic processes using signs to represent objects and generate responses that share understandings, thereby engaging at an intersubjective level to form identities and social roles (Enfield and Kockelman, 2017). Conversely, machines' limited ontological capacities to perceive the material (or social) world prevent them from acting as semiotic agents. Nevertheless, machines are rapidly advancing in these domains, and societal coordination to respond to this reality is urgent (Hui, 2019). To preserve autonomy and interpretive authority while progressing technologically, regulators should design policies that support co-agency with machines without impeding their development (Negarestani, 2018).

3.4. Trade-offs to consider

Trade-offs can be inevitable in this domain. One of them is data minimization versus collection and data sharing. Data sovereignty, as the paper notes, reads the GDPR through its restrictive provisions, such as data minimization and purpose limitation. Data agency reframes the same regulation around portability and data flow. Neither reading is wrong, but they cannot both govern by default, so the prioritization needs a criterion. One such criterion can be the reversibility of harm: where re-identification or downstream misuse would be difficult to undo (health records, biometric data, and anything reachable under transnational data flows). Minimization should govern by default, with sharing requiring an affirmative justification. Where the data are non-personal, aggregated, or protected at the point of use by PETs or generator-verifier architectures, the default should invert: data sharing is acceptable, and restriction requires justification.

This is closer to a sector-based rule than a single criterion, since it tracks the same logic the paper already applies to critical-entity data under the EUCS draft (the sectors carrying the highest

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

re-identification or national-security stakes get the most conservative default, and everything else does not inherit those restrictions by association). The paper's own example of the generator-verifier approach for AI training is the clearest illustration that this need not be zero-sum: the model can be trained "without requiring entities to cede sovereign control," which simplifies the minimization-versus-sharing trade-off rather than choosing a side of it, though that architecture is currently available only for a narrow set of training use cases, not data sharing generally. Nevertheless, coordinating global legal frameworks should continue to be a major priority as well as enforcing them.

A second trade-off raised but not resolved relates to the storage and governance phase: localization versus interoperability. Interoperability should be prioritized for the data spaces and AI-training use cases, particularly due to the finite stock of public training data and the reluctance of firms to share data even though it might have been generated by the public. This suggests that the binding constraint is access to high-quality data, not its location. Yet, data localization should be reserved for critical-entity categories where there is a sovereign risk. For example, Gaia-X-style federation could be combined with the goal of international data spaces and data ecosystems to tackle local, regional, and transnational societal challenges (Bartolomucci et al., 2026).

A final trade-off also highlighted in the subsection above concerns centralization versus decentralization. Large, centralized datasets often improve computational efficiency and model performance but simultaneously concentrate predictive capabilities and market power. Decentralized infrastructures, including federated data spaces, interoperable cloud ecosystems, and distributed identity systems, may sacrifice some efficiency while increasing resilience, competition, and user agency (Mittelstand et al., 2019). Data agency favours decentralization where it redistributes opportunities to participate in data-driven decision-making; however, this requires a degree of sovereignty and control over data as a precondition for meaningful coordination, governance, and enforceability of the law.

Across all three mentioned trade-offs, the underlying prioritization principle the paper supports is: pursue data sovereignty where reversibility is low, and data agency where reversibility is high. Drawing the line is context-dependent; hence, it is yet to be researched which cases warrant one approach or the other and how these approaches should be institutionalized.

4. Discussion

The Westphalian ideal of a state controlling events within borders is fundamentally challenged by a digital economy where predictive power is derived from global, rhizomatic data flows. The European Union's pragmatic pivot towards decentralized technologies that empower data subjects acknowledges this reality. Hence, further work could focus on how to cultivate functional data agency across different contexts. Such an effort requires intensive adaptation and state-led innovation with the input of private actors as well as citizens.

4.1. Data technologies' role in economic global relations and governance

The European Union's regulatory trajectory, analysed through the lens of data agency, reveals a deeper struggle over the politics of time and the architecture of the future. Lyotard (1991, p. 66) explained that economic relations follow the principle that "money is nothing other than time placed in reserve," a stored potential used to "organize the future and neutralize the event" through future guarantees like insurance. This logic of controlling potential events that ought to be paid for by other actors finds its ultimate expression in modern data processing. Today, the world is witnessing the creation of a new layer on top of the economy based on money; one based on abstracted time to fund action to another based on the *data models* (abstracted interpretations to create, predict, and pre-empt the future, whether arbitrary or not). In this context, the highest value lies not in datasets themselves, which cannot easily be priced to be sold, but in the continuous processing of data that can generate actionable intelligence and predictive control over future eventualities.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

A more decentralized, democratic model of data processing increases both humanity and data subjects' agency by seizing the capacity to reassemble time, and not renouncing this opportunity, which is now overly centralized in the hands of a few actors. Instead of a single entity (e.g., a government agency or a large data-driven corporation) which attempts to program the future and foresee eventualities through top-down decision-making and action, decentralized technologies distribute the capacity to set conditions and execute actions across more networks of agents. This pivot moves the discussion beyond the static territoriality of data sovereignty into the dynamic realm of time as the new domain that can better organize capitalism (idealistically speaking). It signifies a recognition that in the digital age, power might no longer be exercised primarily through the control of the distribution of resources through market mechanisms, but also through the governance of time as the predictive capabilities of data technologies, or social coordination as Marx predicted. Data, in this case, might be a resource to tap into.

The governance of two key resources: money and information, and their fusion augments the capacity to model, anticipate and program future events, and when eventualities arrive, to better coordinate and pay for actions to navigate them (Hayek, 1945). Ultimately, this seeks to neutralize uncertainty and systematically organize the future in an increasingly complex world.

In centralized, prominent marketplaces, data trading concentrates this predictive power in the hands of a few dominant platforms. In contrast, the decentralized vision of open-source or the privacy benefits of PETs (when implemented fairly) allows for the creation of data economies that decentralize the "means of prediction" and the capacity to tap into data's capacity to derive meaningful information and monetize it. Beyond the European Union, this vision has also gained popularity in other countries, such as Singapore (Infocomm Media Development (Personal Data Protection Commission, 2020; Authority, 2022; Woods et al., 2023) and across international fora (King, 2022; World Economic Forum, 2022; Jacobson, 2023).

4.2. The future of transatlantic data transfers

The future of data flows, as exemplified by SIGINT, which involves the combination of electronic signals generated from numerous devices, shows that full control over data is complex because data processing is inherently borderless. Nonetheless, E.U. law illustrates that Member States can exercise conditional and legally structured authority over certain data practices. Courts have consistently distinguished between indiscriminate bulk retention—which is prohibited—and targeted, limited retention for national security purposes (Lissens, 2023). This demonstrates that even in a globalized digital environment, the European Union can retain forms of constrained data agency, balancing privacy, surveillance, and security considerations.

Although susceptible to secretive exploitation, mechanisms for participatory oversight and governance frameworks such as the ones introduced by the 2023 Data Privacy Framework can promote dialogue. Multilateral initiatives, like the OECD's *Declaration on Government Access to Personal Data Held by Private Sector Entities* (Organization for Economic Co-operation and Development, 2022), exert normative and diplomatic pressure on governments to adhere to shared standards, increasing transparency and reducing arbitrary access to personal data. Furthermore, the use of PETs across borders is also an option to protect sensitive data (Office of Science and Technology Policy, 2023). Yet, these measures are not neutral: they may inadvertently reinforce existing power imbalances, as resource-rich actors are better positioned to implement and benefit from certain oversight mechanisms and PETs (Veale et al., 2018).

The literature on regulatory interdependence explains that as globalization advances, regulation (or lack thereof) in one jurisdiction affects another (Lazer, 2001). Depending on the policy, distinct types of interdependence emerge. Considering legal clashes between the European Union and the United States, this interdependence should be viewed through how each competes by adopting regulatory approaches that exploit their competitive advantage. The United States has prominent organizations with advanced, diverse data capabilities, enabling superior intelligence and better coordination among stakeholders—key to enhancing agency and global influence. It maintains lower legal standards to safeguard personal data crossing borders, unless it concerns citizens or national security (The White House, 2024).

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

In comparison, the European Union focuses on fundamental rights and attempts to put limits on U.S. companies' data collection activities in the region. At the same time, it actively builds its own technical (Wold, 2024), financial (Carnegie Endowment for International Peace, 2020), and organizational infrastructure to match the capabilities of United States (European Commission, 2024b). Nonetheless, the European Union has also sought to enhance its data agency by strategically benefitting from U.S. intelligence collection efforts, leveraging pragmatic frameworks to access data for its own security. Indeed, as data agency prescribes, the strategic alignment with existing power structures can be leveraged to turn those systems to one's advantage. For example, the e-evidence regulation streamlines cross-border access to electronic data for criminal investigations by enabling law enforcement authorities in the European Union to directly request data from service providers based in the United States (European Union, 2023). This agreement to facilitate electronic evidence access builds upon the U.S. CLOUD Act, which allows Washington to enter into bilateral agreements for direct data access in criminal matters (Department of Justice, 2018). In practice, this demonstrates the E.U. exercising data agency by legally accessing targeted data abroad and leveraging U.S. systems to enhance its security capabilities. By aligning with existing infrastructures, the European Union turns external systems into tools that expand its capacity to act and make informed decisions.

More global cooperation is needed to cultivate collective data agency and handle the world's increasing complexity and interdependence. Information derived from data is essential for increasing humanity's agency, whose full potential can be realized when the insights derived from data-driven analyses are effectively shared, along with the expertise and infrastructure needed to operate the necessary technologies. This would distribute agency and generate what Lévy (1997) termed "collective intelligence."

Nonetheless, regarding SIGINT—a key issue surrounding the E.U.–U.S. data transfer negotiations—the fusion of trillions of signals combined with the analytical capabilities of AI creates a panoramic level of information awareness that can be readily abused. Those who wield this power can intervene across a wide range of tempting policy domains to gain an advantage. This raises questions about the distinction between data agency and data power. Data analysis can be used to achieve common goals such as the anticipation of threats, but it can also be exploited for less benign objectives. In this regard, the proposed but withdrawn 2017 ePrivacy Regulation to complement the GDPR intended to play a major legal role in the protection of electronic communications (European Union, 2017). After years of stalled negotiations and mounting criticism, the ePrivacy Regulation proposal was abandoned in 2025 after critics argued it was unrealistic in its ambitions, attempting to address a broad spectrum of complex issues, ranging from cookie consent to metadata protection, in a single legislative act (Andrews, 2025).

4.3. Policy implications

A regulatory framework that genuinely empowers data agency must, therefore, focus on architectures and rights that protect and enhance data subjects' agency and sovereignty for greater self-determination and interpretive authority and capabilities over the data that they generate. The European Union has already established this framework with the GDPR (European Commission, 2026). Step one is to make existing rights enforceable in practice, not just on paper. Enforcement requires three concrete actions: common technical formats so a portability request produces usable data, binding timelines with penalties for non-compliance comparable to other GDPR enforcement, and cohesion among data protection authorities. This allows individuals to stop being passive data sources (NOYB, 2025).

In the storage and governance phases, data sovereignty stresses cybersecurity and local compliance, possibly including localization (Blancato, 2024). Data agency favours scalable, interoperable storage for collaborative access. A balanced approach includes hybrid, multi-cloud, federated (e.g., Gaia-X), and local storage for sensitive data, alongside global solutions for computational power. The two approaches together are needed as they directly contest the centralization of data processing activities and the capacity to draw information. Nevertheless, the growth of local CSPs is extremely important to fulfil the Commission's goal of increasing resilience in the face of unforeseen circumstances and for adopting a diversified multi-cloud strategy (European Commission, 2019a).

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

In the analysis and use phases, designing systems that augment human intelligence rather than replace it, fostering shared representations for clearer communication (Heer, 2019), and cultivating high digital literacy can empower users to interrogate models and engineer them. Here, testing innovative processing methods in controlled environments (sandboxes) can support compliance learning (Allen, 2019).

5. Conclusion

As data technologies increasingly shape human life, societies face a choice: to engage with the results of data processing activities to enhance their agency or to relinquish it. This article has sought to contribute to the development of the concept of data agency to advance alternative but pragmatic and forward-looking frameworks for understanding the growing influence of data-driven technologies and the regulatory efforts that respond to them. To cover these conceptual blind spots, *data agency* explains how, not through hermetic control but through cultivating collective cooperation via fairer data relations and decentralized technologies that empower individuals, may allow them to make more informed decisions and take effective action in informing policymaking for tackling societal challenges. The European strategy for data embraces innovation through regulation while remaining flexible enough to take advantage of the latest technological advancements produced elsewhere, especially those associated with AI and cloud computing. Nevertheless, it is undeniable that a lack of control over data can hinder an agent's ability to cultivate data agency. Thus, the European Union is expected to continue struggling to balance the strategic integration of data-driven technologies with the development of robust infrastructure to support their scaling.

Data availability statement. This article does not generate or analyse new datasets. The arguments and analysis presented are conceptual and informed by existing literature, policy documents, and the author's professional experience in the field of data governance and digital policy. No primary or secondary data requiring deposition in a public repository were used in this study.

Acknowledgements. The author is thankful to Iryna Susha, Koen Frenken, Alessio Tartaro, and Jorge Igareda for their input and support.

Author contribution. Conceptualization: J.B.; Data curation: J.B.; Formal analysis: J.B.; Funding acquisition: J.B.; Investigation: J.B.; Methodology: J.B.; Project administration: J.B.; Resources: J.B.; Software: J.B.; Supervision: J.B.; Validation: J.B.; Visualization: J.B.; Writing – original draft: J.B.; Writing – review & editing: J.B.

Funding statement. The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Dutch Research Council (NWO) under the grant agreement VI.Vidi.221R.021. Open access funding provided by Utrecht University.

Competing interests. The authors declare none.

References

Adler-Nissen R and Eggeling KA (2024) The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *JCMS: Journal of Common Market Studies 62*(4), 993–1011. https://doi.org/10.1111/jcms.13594.

Allen HJ (2019) Regulatory sandboxes. *George Washington Law Review 87*, 579 Available at https://digitalcommons.wcl.american.edu/facsch_lawrev/709 (accessed 26 December 2025).

Amazon Web Services (2022) *Europe Digital Sovereignty.* Available at https://aws.amazon.com/compliance/europe-digital-sovereignty/ (accessed 26 December 2025).

Andrejevic M (2014) Big data, big questions: The big data divide. *International Journal of Communication 8*, 17. Available at https://ijoc.org/index.php/ijoc/article/view/2161.

Andrews C (2025) European Commission withdraws AI Liability Directive from Consideration. International Association of Privacy Professionals. Available at https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration/ (accessed 26 December 2025).

Badiou A (2006) *Being and Event*. London: Bloomsbury Academic. https://doi.org/10.5040/9781350252035.

Barker T (2020) Breaking the Transatlantic Data Trilemma: The EU must Step Up Its Approach to EU-US Data Flows (DGAP Policy Brief No. 27). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. Available at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-71281-8 (accessed 26 December 2025).

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Bartolomucci F, **Ramalli E and Urbano VM** (2026) Integrated governance in data ecosystems: A conceptual framework consolidating collaborative and data governance. *Government Information Quarterly 43*(1), 102107. https://doi.org/10.1016/j.giq.2026.102107.

Bauer M (2023) Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements (ECIPE Policy Brief No. 01/2023). Available at https://ecipe.org/wp-content/uploads/2023/10/ECI_23_OccasionalPaper_04-2023_LY06.pdf (accessed 26 December 2025).

Bauer M and Lamprecht P (2023) The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States (ECIPE Occasional Paper No. 04/2023). Available at https://ecipe.org/publications/eucs-immunity-requirements-economic-impacts/ (accessed 26 December 2025).

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society 11*(6), 985–1002. https://doi.org/10.1177/1461444809336551.

Bernal J (2024) Private sector trust in data sharing: Enablers in the European Union. *Data & Policy 6*, e30. https://doi.org/10.1017/dap.2024.20.

Blancato FG (2024) The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet 16*(1), 12–32. https://doi.org/10.1002/poi3.358.

Blind K, **Niebel CM and Rammer C** (2022) The Impact of the EU General Data Protection Regulation on Innovation in Firms (ZEW Discussion Paper No. 22–047). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4257740 (accessed 26 December 2025).

Butler J, **Laclau E and Žižek S** (2000) *Contingency, Hegemony, Universality: Contemporary Dialogues on the Left*. London: Verso.

Carnegie Endowment for International Peace (2020) *Europe and AI: Leading, Lagging behind, or Carving Its Own Way?* Available at https://carnegieendowment.org/research/2020/07/europe-and-ai-leading-lagging-behind-or-carving-its-own-way?lang=en (accessed 26 December 2025).

Center for Strategic and International Studies (2023) *European Cybersecurity Certification Scheme for Cloud Services.* Available at https://www.csis.org/analysis/european-cybersecurity-certification-scheme-cloud-services (accessed 26 December 2025).

Chander A and Sun H (eds) (2023) *Data Sovereignty: From the Digital Silk Road to the Return of the State*. New York: Oxford University Press. https://doi.org/10.1093/oso/9780197582794.001.0001.

Chee FY (2024) EU Cybersecurity Label Should Not Discriminate Against Big Tech, European Groups Say. *Reuters.* Available at https://www.reuters.com/technology/cybersecurity/eu-cybersecurity-label-should-not-discriminate-against-big-tech-european-groups-2024-06-17/ (accessed 26 December 2025).

Couldry N (2014) Inaugural: A necessary disenchantment: Myth, agency and injustice in a digital world. *The Sociological Review 62*(4), 880–897. Available at https://doi.org/10.1111/1467-954X.12158 (accessed 26 December 2025).

Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society 1*(2). https://doi.org/10.1177/2053951714539277.

De Hert P and Boulet G (2013) *Cloud Computing and Trans-Border Law Enforcement Access to Private Sector Data: Challenges to Sovereignty, Privacy and Data Protection.* In Workshop paper collection: 'Big data & privacy. Making ends meet' (pp. 23–26). Future of Privacy Forum and Center for Internet and Society at Stanford Law School. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2530465 (accessed 26 December 2025).

Department of Defense (1981) Executive Order 12333 of December 4, 1981, 46 Fed. Reg. 59941. Available at https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf (accessed 26 December 2025).

Department of Justice (2018) *Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018*, Pub. L. No. 115–141, 132 Stat. 1213. Available at https://www.justice.gov/criminal/media/999391/dl?inline (accessed 31 July 2026).

Devlin J Chang M, **Lee K and Toutanova K** (2018) *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.* In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL-HLT).* Available at https://doi.org/10.48550/arXiv.1810.04805 (accessed 26 December 2025).

DIGITALEUROPE (2022) *Data Transfers in the Data Strategy: Understanding Myth and Reality.* Available at https://cdn.digitaleurope.org/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf (accessed 26 December 2025).

Emirbayer M and Mische A (1998) What is agency? *American Journal of Sociology 103*(4), 962–1023. https://doi.org/10.1086/231294.

Enfield NJ and Kockelman P (eds) (2017) *Distributed Agency.* New York: Oxford University Press.

European Commission (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (accessed 26 December 2025).

European Commission (2019a) *The European Commission Cloud Strategy: Cloud as an Enabler for the European Commission Digital Strategy.* Available at https://commission.europa.eu/document/download/3bb440ec-f777-484c-8802-baf08ebb87c0_en?filename=ec_cloud_strategy.pdf (accessed 26 December 2025).

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

European Commission (2020a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* (COM(2020) 66). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066 (accessed 26 December 2025).

European Commission (2020b) *Open Source Software Strategy 2020–2023: Think Open (Communication C(2020) 7149 final).* European Commission. Available at https://commission.europa.eu/system/files/2020-10/en_ec_open_source_strategy_2020-2023.pdf (accessed 26 December 2025).

European Commission (2021) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: The European Way for the Digital Decade.* Available at https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed 26 December 2025).

European Commission (2022) *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act).* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854&qid=1733478604733 (accessed 26 December 2025).

European Commission. (2023a). *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance).* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854&qid=1733478604733 (accessed 26 December 2025).

European Commission (2023b) *Commission implementing decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework.* Available at https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (accessed 26 December 2025).

European Commission (2024a) *Report from the Commission to the European Parliament and the Council on the First Periodic Review of the Functioning of the Adequacy Decision on the EU-US Data Privacy Framework.* Available at https://commission.europa.eu/document/download/25695177-8073-4ce3-bf81-eb816dc6b468_en?filename=Report%20on%20the%20first%20periodic%20review%20of%20the%20functioning%20of%20the%20adequacy%20decision%20on%20the%20EU-US%20Data%20Privacy%20Framework.pdf (accessed 26 December 2025).

European Commission (2024b) *Niinistö Report: Proposal for an EU Intelligence Agency.* Available at https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf (accessed 26 December 2025).

European Commission (2026) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, Accompanied by an EU Open Source Strategy* (COM(2026) 503 Final). Available at https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy (accessed 17 June 2026).

European Data Protection Board (2023) *1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision.* Available at https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en#:~:text=Brussels%2C%2022%20May%20%2D%20Following%20the,Protection%20Authority%20(IE%20DPA) (accessed 26 December 2025).

European Data Protection Board (2024) *Report on the First Review of the EU-US Data Privacy Framework.* Available at https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf (accessed 26 December 2025).

European Union (1992/2007) Consolidated version of the treaty on European Union. *Official Journal of the European Union 326*, 13–390 Available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (accessed 26 December 2025).

European Union (2017) *Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010 (accessed 26 December 2025).

European Union (2023) *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543 (accessed 26 December 2025).

European Union Agency for Cybersecurity (2020) *EUCS – Cloud Services Scheme EUCS, a Candidate cybersecurity certification Scheme for Cloud Services* (December 2020). Available at https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf (accessed 26 December 2025).

Farrell E, **Minghini M**, **Kotsev A**, **Soler Garrido J**, **Tapsall B**, **Micheli M**, **Posada Sánchez M**, **Signorelli S**, **Tartaro A**, **Bernal Cereceda J**, **Vespe M**, **Di Leo M**, **Carballa-Smichowski B**, **Smith R**, **Schade S**, **Pogorzelska K**, **Gabrielli L and de Marchi D** (2023) *European Data Spaces—Scientific Insights into Data Sharing and Utilisation at Scale* (JRC Report No. JRC129900). Joint Research Centre. https://doi.org/10.2760/400188

Farrell H and Newman A (2016) The new interdependence approach: Theoretical development and empirical demonstration. *Review of International Political Economy 23*(5), 713–736. https://doi.org/10.1080/09692290.2016.1247009.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Farrell H and Newman AL (2019) *Of Privacy and Power: The Transatlantic Struggle over Freedom and security.* Princeton: Princeton University Press.

Farrell H and Newman A (2023) *Underground Empire: How America Weaponized the World economy.* Henry Holt and Co.

Foucault M (1978) *The History of Sexuality: Volume I: An Introduction* (R. Hurley, Trans.). New York: Pantheon Books.

Gaia-X (2024) *Gaia-X General Overview.* Available at https://gaia-x.eu/wp-content/uploads/2024/10/20240625_Gaia-X-standard-Presentation.pdf (accessed 26 December 2025).

Gal MS and Aviv O (2020) The competitive effects of the GDPR. *Journal of Competition Law & Economics 16*(3), 349–391. https://doi.org/10.1093/joclec/nhaa012. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444 (accessed 26 December 2025).

Google Cloud (2022) *Advancing Digital Sovereignty on Europe's Terms.* Available at https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms (accessed 26 December 2025).

Hansen M (2024) From attention economy to cognitive lock-ins. *Big Data & Society 11*(3). https://doi.org/10.1177/20539517241275878.

Hayek FA (1945) The use of knowledge in society. *The American Economic Review 35*(4), 519–530 Available at http://www.jstor.org/stable/1809376 (accessed 20 June 2026).

Heer J (2019) Agency plus automation: Designing artificial intelligence into interactive systems. *Proceedings of the National Academy of Sciences*, *116*(6), 1844–1850. Available at https://doi.org/10.1073/pnas.1807184115 (accessed 26 December 2025).

Hellmeier M and von Scherenberg F (2023) *A Delimitation of Data Sovereignty from Digital and Technological Sovereignty.* In *ECIS 2023.* Available at https://aisel.aisnet.org/ecis2023/ (accessed 26 December 2025).

Hui Y (2019) *Recursivity and Contingency.* London: Rowman & Littlefield Publishers.

Hummel P, **Braun M**, **Tretter M and Dabrock P** (2021) Data sovereignty: A review. *Big Data & Society 8*(1). https://doi.org/10.1177/2053951720982012.

Hurtado Ramírez D, **Porras Díaz L**, **Rahimian S**, **Auñón García JM**, **Irigoyen Peña B**, **Al-Khazraji Y**, **Gavín Alarcón Á**, **González Fuente P**, **Soler Garrido J and Kotsev A** (2023) *Technological Enablers for Privacy Preserving Data Sharing and Analysis* (No. JRC134350). Joint Research Centre (Seville site). 978-92-68-06693-5 (online) (accessed 26 December 2025).

Infocomm Media Development Authority (2022) *Invitation to Participate in Privacy Enhancing Technology Sandbox "PET Sandbox."* Available at https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/pet-sandbox-cfp.pdf (accessed 26 December 2025).

International Data Spaces Association (2025) *Why Data Spaces Should Anchor the EU's Data Union Strategy.* Available at. https://internationaldataspaces.org/why-data-spaces-should-anchor-the-eus-data-union-strategy/ (accessed 26 December 2025).

Irion K (2012) Government cloud computing and national data sovereignty. *Policy & Internet 4*(3–4), 40–71. https://doi.org/10.1002/poi3.10.

Jacobson J (2023) The Impact of Privacy-Enhancing Technologies (PETs) on Business, Individuals and Society. World Economic Forum. Available at https://www.weforum.org/stories/2023/10/the-impact-of-privacy-enhancing-technologies-pet-on-business-individuals-and-society/ (accessed 26 December 2025).

Johnson RL, **Pistilli G**, **Menédez-González N**, **Duran LDD**, **Panai E**, **Kalpokiene J and Bertulfo DJ** (2022) *The Ghost in the Machine Has an American Accent: Value Conflict in GPT-3*. https://doi.org/10.48550/arXiv.2203.07785

Kant I (1785/2011) Zweyter Abschnitt / Second Section. In Gregor M, Timmermann J and Kant I(eds), *Groundwork of the Metaphysics of Morals: A German–English Edition* Cambridge: Cambridge University Press,(pp. 40–119.

Kasy M (2025) *The Means of Prediction: How AI Really Works (and Who Benefits)*. Chicago: University of Chicago Press.

Kennedy H, **Poell T and van Dijck J** (2015) Data and agency. *Big Data & Society 2*(2). https://doi.org/10.1177/2053951715621569.

King R (2022) Web3: The Hype and How It Can Transform the Internet. World Economic Forum. Available at https://www.weforum.org/stories/2022/02/web3-transform-the-internet/ (accessed 26 December 2025).

Krasner SD (2001) Rethinking the sovereign state model. *Review of International Studies 27*(5), 17–42. https://doi.org/10.1017/S0260210501008014.

Laclau E and Mouffe C (1985) *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso.

Latour B (1999) *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, Massachusetts, Harvard University Press.

Lazer D (2001) Regulatory interdependence and international governance. *Journal of European Public Policy 8*(3), 474–492. https://doi.org/10.1080/13501760110056077.

Lévy P (1997) *Collective Intelligence: Mankind's Emerging World in Cyberspace*. Cambridge, Massachusetts, Perseus Books.

Li I, **Dey A and Forlizzi J** (2010) A Stage-Based Model of Personal Informatics Systems. *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, CHI 2010, Atlanta, Georgia, USA, April 10-15, 2010, 557–566.

Lissens S (2023) EU-US Data Flows and Data Transfers in Crisis: How to Move Forward? In Catolica Graduate Legal Research Conference 2023: Law and Crises. Catolica University, Lisbon. Available at https://ghum.kuleuven.be/ggs/wp238-sylvialissens.pdf (accessed 26 December 2025).

Lynskey O (2019) Grappling with "data power": Normative nudges from data protection and privacy. *Theoretical Inquiries in Law 20*(1), 189–220. https://doi.org/10.1515/til-2019-0007.

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Lyon D (2014) Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society 1*(2), 2053951714541861.

Lyotard JF (1991) *The Inhuman: Reflections on Time*. Stanford: Stanford University Press.

March C and Scieferdecker I (2023) Technological sovereignty as ability, not autarky. *International Studies Review 25*(2). https://doi.org/10.1093/isr/viad012.

Marquis P (2024) *FISA Section 702 Reauthorized for Two Years.* Available at https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years (accessed 26 December 2025).

Microsoft (2022) *Microsoft Cloud for Sovereignty: The Most Flexible and Comprehensive Solution for Digital Sovereignty.* Available at https://blogs.microsoft.com/blog/2022/07/19/microsoft-cloud-for-sovereignty-the-most-flexible-and-comprehensive-solution-for-digital-sovereignty/ (accessed 26 December 2025).

Mittelstadt B, **Russell C and Wachter S** (2019) *Explaining Explanations in AI.* Proceedings of the conference on fairness, accountability, and transparency, 279–288. https://link.springer.com/book/10.1007/978-981-95-3811-9.

Mueller ML (2020) Against sovereignty in cyberspace. *International Studies Review 22*(4), 779–801. https://doi.org/10.1093/isr/viz044.

Negarestani R (2018) *Intelligence and Spirit*. Massachusetts, Urbanomic, MIT Press.

NOYB (2025) *Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission* (Version 1.0). Available at https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf (accessed 26 December 2025).

Office of Science and Technology Policy (2023) *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics: A Report by the Fast-Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics Networking and Information Technology Research and Development Subcommittee.* National Science and Technology Council. Available at https://www.nitrd.gov/pubs/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf (accessed 26 December 2025).

Organisation for Economic Co-operation and Development (2022) *Declaration on Government Access to Personal Data Held by Private Sector Entities.* Available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 (accessed 26 December 2025).

OVHcloud (2022) *Sovereign Cloud.* Available at https://www.ovhcloud.com/en/about-us/sovereign-cloud/ (accessed 26 December 2025).

Personal Data Protection Commission (2020) *Guide to Managing Data Intermediaries. Personal Data Protection Commission.* Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Intermediaries–2020.pdf (accessed 26 December 2025).

Pohle J and Thiel T (2020) Digital sovereignty. *Internet Policy Review 9*(4). https://doi.org/10.14763/2020.4.1532.

Polatin-Reuben D and Wright J (2014) An internet with {BRICS} characteristics: Data sovereignty and the balkanisation of the internet. *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14) 25*(2). https://doi.org/10.1093/isr/viad012.

Přibáň J (2015) The semantics of constitutional sovereignty in post-sovereign "new" Europe: A case study of the Czech constitutional court's jurisprudence. *International Journal of Constitutional Law 13*(1), 180–199. https://doi.org/10.1093/icon/mov008.

Rikap C, **Durand C**, **Paraná E**, **Gerbaudo P and Marx P** (2024) *Reclaiming Digital Sovereignty: A Roadmap to Build a Digital Stack for People and the Planet.* Available at https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/reclaiming-digital-sovereignty.pdf (accessed 26 December 2025).

Saeed W and Omlin C (2023) Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities. *Knowledge-Based Systems 263*, 110273. https://doi.org/10.1016/j.knosys.2023.110273.

Samek W, **Montavon G**, **Lapuschkin S**, **Anders CJ and Müller KR** (2021) Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE 109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483.

Sharma A, **Rao S**, **Brockett C**, **Malhotra A**, **Jojic N and Dolan B** (2024) *Investigating Agency of LLMs in Human-AI Collaboration Tasks.* In Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics (Volume 1: Long Papers) (pp. 1968–1987). Association for Computational Linguistics. Available at https://aclanthology.org/2024.eacl-long.119/ (accessed 26 December 2025).

Siddiq F, **Røkenes FM**, **Lund A and Scherer R** (2024) New kid on the block? A conceptual systematic review of digital agency. *Education and Information Technologies 29*(5), 5721–5752. https://doi.org/10.1007/s10639-023-12038-3.

Susha I, **Schiele J and Frenken K** (2022) *Business-to-Government Data Sharing for Public Interests in the European Union: Results of a Public Consultation*. In *International Conference on Electronic Government*. Cham: Springer International Publishing, pp. 515–529. https://doi.org/10.1007/978-3-031-15086-9_33.

Swire P, **Kennedy-Mayo D**, **Bagley D**, **Krasser S**, **Modak A and Bausewein C** (2024) Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy 9*(1), 20–51. https://doi.org/10.1080/23738871.2024.2384724.

Synergy Group (2020) *Amazon and Microsoft Lead the Cloud in All Major European Countries.* Available at https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries (accessed 26 December 2025).

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.

Synergy Research Group (2022) *European Cloud Providers Continue to Grow but Still Lose Market Share.* Available at https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share (accessed 26 December 2025).

Tausch A (2010) Globalisation and development: The relevance of classical "dependency" theory for the world today. *International Social Science Journal 61*(202), 467–488. https://doi.org/10.1111/j.1468-2451.2011.01786.x.

The White House (2022) *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework.*

The White House (2024) *Fact Sheet: President Biden Issues Sweeping Executive Order to Protect Americans' Sensitive Personal Data*.

Tracol X (2020) Schrems II: The return of the privacy shield. *Computer Law & Security Review 39*, 105484. https://doi.org/10.1016/j.clsr.2020.105484.

United States (1978) *Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c.* Available at https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf (accessed 26 December 2025).

United States (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)*, Pub. L. No. 107–56, 115 Stat. 272. Available at https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (accessed 26 December 2025).

Vartiainen H, **Pellas L**, **Kahila J**, **Valtonen T and Tedre M** (2024) Pre-service teachers' insights on data agency. *New Media & Society 26*(4), 1871–1890. https://doi.org/10.1177/14614448221079626.

Veale M, **Binns R and Ausloos J** (2018) When data protection by design and data subject rights clash. *International Data Privacy Law 8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002.

Villalobos P, **Ho A**, **Sevilla J**, **Besiroglu T**, **Heim L and Hobbhahn M** (2024) Position: Will we run out of data? Limits of LLM scaling based on human-generated data. *Proceedings of the 41st International Conference on Machine Learning*, *235*, 49523–49544. Proceedings of Machine Learning Research (PMLR). https://proceedings.mlr.press/v235/villalobos24a.html

Wold JW (2024) *Von der Leyen Gives Nod to €100 Billion CERN for AI Proposal.* Euractiv, July 25.Available at https://www.euractiv.com/section/digital/news/von-der-leyen-gives-nod-to-e100-billion-cern-for-ai-proposal/ (accessed 26 December 2025).

Woods O, **Bunnell T and Kong L** (2023) The state-led platformisation of financial services: Frictionless ecosystems and an expansive logic of "smartness" in Singapore. *Geoforum 146*, 103849. https://doi.org/10.1016/j.geoforum.2023.103849.

Wooldridge M and Jennings NR (1995) Intelligent agents: Theory and practice. *The Knowledge Engineering Review 10*(2), 115–152. https://doi.org/10.1017/S0269888900008122.

World Economic Forum (2022) *Advancing Digital Agency: The Power of Data Intermediaries (Insight Report).* https://www3.weforum.org/docs/WEF_Advancing_towards_Digital_Agency_2022.pdf (accessed 26 December 2025).

Cite this article: Bernal J (2026). Advancing data agency: A conceptual framework to support data sovereignty. *Data & Policy*, 8: e44. doi:10.1017/dap.2026.10089

Downloaded from https://www.cambridge.org/core. 13 Nov 2026 at 10:54:19, subject to the Cambridge Core terms of use.