U.C.L.A. Law Review

Sovereignty and the Governance of Artificial Intelligence

Teresa Scassa

ABSTRACT

This Essay explores the concept of sovereignty in relation to artificial intelligence. Although sovereignty has long been used to describe the status of nation states, the concept of sovereignty is used in multiple ways in the digital context. It is used to articulate state policies in relation to artificial intelligence (AI) and data, an assertion of state sovereignty that often has extraterritorial effects. It is also used by many Indigenous communities to articulate the relevance of control over data—in a data-driven world—to self-determination. The concept of sovereignty is also applied to describe the relationship of individuals to both data and technology, and in this sense, it is meant to highlight the importance of individual control over the defining elements of self. The concept of sovereignty clearly speaks to ideas of autonomy and control and takes on particular importance in a context in which AI technologies challenge these concepts in novel ways. This Essay explores the shifting concept of sovereignty and examines what it means for the regulation of AI, paying particular attention to the data dimensions of AI.

AUTHOR

Dr. Teresa Scassa is the Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law where she is also a member of the Centre for Law, Technology and Society. Teresa's research addresses digital and data governance issues. She currently sits on Canadian Advisory Council on Artificial Intelligence and has also served as Scholar-in-Residence at the Ontario Information and Privacy Commissioner's office. She is a co-editor of the books AI and the Law in Canada (2021), Law and the Sharing Economy (2017), and The Future of Open Data (2022). She is co-author of Digital Commerce in Canada (2020) and Canadian Intellectual Property Law (2022).

TABLE OF CONTENTS

INTRODUCTION

In international law, sovereignty is a concept that supports a nation state's authority to act autonomously with respect to matters within its own borders. Sovereignty is a justification for state action to govern artificial intelligence (AI) even though, like other digital technologies, AI transcends national boundaries. At the same time, in a context where control and autonomy may be undermined or enabled by technology, we see the language of sovereignty reshaped and adapted to describe new relationships involving subnational entities, groups and even individuals. This Essay explores the shifting concept of sovereignty and examines what it means for the regulation of AI, paying particular attention to the data dimensions of AI.

Sovereignty is principally a concept used in relation to nation states. Although it has been considerably battered by the forces of technology and globalization,[1] the state remains the principal entity of governance, even though the once near-absolute power of the state is now moderated by international agreements. This Essay does not focus on the Westphalian notion of sovereignty as an exercise of exclusive territorial jurisdiction;[2] rather it explores a broader concept of sovereignty as a way of thinking about the governance of technology, including AI. Part I considers the manifestations of digital sovereignty—a state's power to assert control in the digital realm—a concept already shaping contemporary AI governance. Part II explores the idea of sovereignty as a claim which focuses on the dynamics of relationships and the application of this approach in the AI context. Part III examines what some of those different sovereignties are and how they may impact the nature and location of AI governance.

I. DIGITAL SOVEREIGNTY

Digital sovereignty is a term increasingly used in the sphere of technology policy. In their paper on digital sovereignty, technology law professors Anupam Chander and Haochen Sun define it as "the application of traditional state

1. JAN AART SCHOLTE, GLOBALIZATION: A CRITICAL INTRODUCTION 188–92 (2d ed. 2005).
2. *See id.* at 188 (describing this as a context where "each state would exercise supreme, comprehensive, unqualified and exclusive rule over its territorial jurisdiction").

sovereignty over the online domain."[3] On one level, digital sovereignty maps well onto conventional state sovereignty goals. For example, a U.S. Congressional Research Service report described digital sovereignty as an increasingly important concern in the European Union (EU).[4] The report stated that EU member nations defined digital sovereignty as the ability "to act independently on the world stage, exerting leadership in line with EU interests and values."[5] Yet Chander and Sun note that digital sovereignty has important differences from conventional state sovereignty. They outline four distinct features of digital sovereignty:

> [D]igital sovereignty can create significant roadblocks to one of the internet's key virtues–its empowering of global connections. Second, because the digital sphere is intermediated by corporations, the assertion of digital sovereignty typically occurs vis-à-vis corporations, not governments. Third, because our lives are increasingly permeated by the internet, digital sovereignty can offer governments surveillance tools that far exceed any history has previously provided. Fourth, because of the dominance of U.S. technology companies globally, governments can readily weaponize digital sovereignty to serve protectionist goals.[6]

Digital sovereignty is thus not just about a nation's right to chart its own course within the parameters of international law. It also describes the ability to exercise unique power over corporations, individuals, and even other states via the increasingly indispensable technological infrastructure that shapes our lives. For these reasons, Chander and Sun describe digital sovereignty as "both necessary and dangerous."[7]

The history of sovereignty is a history of control and influence over others.[8] Digital sovereignty is no different. The transformational nature of AI and its potential to drive economic, scientific, and technological dominance, means that

3. Anupam Chander & Haochen Sun, *Sovereignty 2.0*, GEO. L. FAC. PUBL'NS & OTHER WORKS, 2021 at 1, 10. Note that technology philosopher Professor Luciano Floridi uses a somewhat different approach when he defines digital sovereignty in terms of control "of *data*, *software* (e.g. AI), *standards* and *protocols* (e.g. 5G, domain names), *processes* (e.g. cloud computing), *hardware* (e.g. mobile phones), *services* (e.g. social media, e-commerce), and *infrastructures* (e.g. cables, satellites, smart cities)." Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHIL. & TECH. 369, 370–71 (2020).
4. RACHEL F. FEFER, CONG. RSCH. SERV., R46732, EU DIGITAL POLICY AND INTERNATIONAL TRADE 2 (2021).
5. *Id.* at 3; *see also* Chander & Sun, *supra* note 3, at 15–16 (stating that even within the EU, individual states such as Germany and France are asserting forms of sovereignty).
6. Chander & Sun, *supra* note 3, at 21.
7. *Id.* at 8.
8. PETER H. RUSSELL, SOVEREIGNTY: THE BIOGRAPHY OF A CLAIM 10 (Univ. Toronto Press 2021).

there is a race to control, or at least influence, the norms and standards that will govern it.[9] The EU has formed a powerful political bloc that has had considerable success in shaping data protection law through a combination of relatively swift and concerted actions with significant extraterritorial effect.[10] Indeed, the "Brussels effect"[11] is evident in the impact of the Data Protection Directive[12] and later the General Data Protection Regulation (GDPR)[13] which prompted some countries to enact or modify data protection laws and led to the development of the Privacy Shield in the United States.[14] AI regulation is part of the broader EU technology regulation agenda,[15] and the AI Act[16] is poised to have extraterritorial impacts similar to those of the GDPR.[17]

China, another notable world power, has taken steps to exercise its own digital sovereignty. Through a variety of measures, they have regulated the behavior of its citizens and digital actors within its borders.[18] Chander & Sun describe China's approach to digital sovereignty as "multifaceted,"[19] including "controlling its physical infrastructure, regulating content, balancing negative economic impacts, and building international support for its conceptions of data sovereignty."[20] China also exercises soft power through its provision of technology

9. *See, e.g.*, Nathalie A. Smuha, *From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence*, 13 L. INNOVATION & TECH. 57 (2021).
10. *See, e.g.*, 1995 O.J. (L 281) [hereinafter Protection of Individuals Regulation]. This was followed by 2016 O.J. (L 119) [hereinafter Protection of Natural Persons Regulation] and 2018 O.J. (L 127) [hereinafter General Data Protection Regulation]. Chander and Sun posit that the nature of the internet means that extraterritorial impact is a feature of digital sovereignty. Chander & Sun, *supra* note 3, at 22.
11. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2012). The "Brussels effect" is a term coined to refer to the extraterritorial harmonizing impact of EU regulations through the market power exerted by the EU.
12. Protection of Individuals Regulation, *supra* note 10.
13. Protection of Natural Persons Regulation, *supra* note 10; General Data Protection Regulation, *supra* note 10.
14. PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome [https://perma.cc/ J55Z-JGPV].
15. *See* 2022 O.J. (L 265); 2022 O.J. (L 277); General Data Protection Regulation, *supra* note 10.
16. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).
17. General Data Protection Regulation, *supra* note 10.
18. *The Internet in China, Information Office of the State Council of the People's Republic of China*, USC US-CHINA INST. (June 8, 2010), https://china.usc.edu/prc-state-council-internet-china-june-8–2010 [https://perma.cc/S9WF-AW7Q]; *see also* Chander & Sun, *supra* note 3, at 11–15.
19. Chander & Sun, *supra* note 3, at 11.
20. *Id.*

infrastructure and innovation in non-Western nations.[21] Russia has its own digital sovereignty agenda, focused primarily on control over what its nationals see or do, which depends upon the state control of infrastructure.[22] Both Russia and China reject Western technological dominance and the associated ideology. In both cases, law and policy are also intended to strengthen domestic technological and innovative capacity. In the case of AI, the Organization for Economic Cooperation and Development (OECD) has noted that a stable policy environment is needed "to foster trust in and adoption of AI and society."[23] Policymaking takes place on a global stage where normative and regulatory dominance are closely linked to economic and technological dominance as well.[24] Within the traditional concept of sovereignty, therefore, control over digital technologies is seen as crucial to internal and external state powers. Many states are regulating these technologies accordingly.[25]

Digital governance can serve both domestic and international goals. For example, in introducing Canada's recent bill to enact the Artificial Intelligence and Data Act,[26] the Minister of Industry stated that Canada would become "one of the first countries in the world to create a framework for the responsible use of artificial intelligence."[27] Such a claim can be understood both in terms of Canada's aspirations to compete in the international AI arena[28] and as an assertion of digital

21. *Id.* at 14–15.
22. *Id.* at 16–17; Gavin Wilde & Justin Sherman, *Putin's Internet Plan: Dependency With a Veneer of Sovereignty*, TECHSTREAM (May 11, 2022), https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty [https://perma.cc/2ZYJ-LSPD].
23. OECD, *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, "Background Information,"* OECD LEGAL INSTRUMENTS (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#backgroundInformation [https://perma.cc/PE7M-LCUS].
24. FEFER, *supra* note 4, at 1.
25. For a review of international approaches to AI regulation, see Michael Geist, *AI and International Regulation*, *in Artificial Intelligence and the Law in Canada* 367 (Florian Martin-Bariteau & Teresa Scassa ed., LexisNexis 2021); ANTHEM PRESS, INTERNATIONAL PERSPECTIVES ON ARTIFICIAL INTELLIGENCE (J. Mark Munoz & Alka Maurya eds., 2022); *see also* Chander & Sun, *supra* note 3.
26. *Digital Charter Implementation Act*, 44th Parliament (2022) (Can.).
27. François-Philippe Champagne, Minister of Innovation, Sci. & Indus., House of Commons Debates (Nov. 4, 2022) (transcript available at https://www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-125/hansard) [https://perma.cc/D2QC-RL6G]).
28. For a discussion of Canadian investments in AI, see Council of Canadian Academies, Leaps and Boundaries: The Expert Panel on Artificial Intelligence for Science and Engineering 16–17 (2022), https://cca-reports.ca/wp-content/uploads/2022/05/Leaps-and-Boundaries_FINAL-DIGITAL.pdf [https://perma.cc/VRR7-9H68].

sovereignty. AI governance is therefore both an internal normative act and the staking of an international claim to power.

In this vision of digital sovereignty, the nation state is the key actor in a context where power is also wielded by other actors. International organizations wield power through treaties. Multinational corporations do the same through internal policies, codes of conduct and other voluntary instruments. But among these actors, only nations exercise sovereignty in the political sense. Nations can and do act through international organizations, often making concessions that limit future actions in exchange for certain benefits, such as policy concessions made in the interest of international trade.[29] Corporations may volunteer to self-govern—and may bring to bear considerable pressure on national governments to allow them to do so—although they ultimately remain subject to laws and regulations.[30]

II. A DIFFERENT KIND OF SOVEREIGNTY

Sovereignty is a concept that has broad political and social dimensions. It is capable of a complexity of meaning. As I use it here, sovereignty is more than national authority and legislative competence vis à vis other nations. Undoubtedly, this more nuanced notion of sovereignty is intertwined in any discussion of AI governance. In his recent book on sovereignty, political scientist Peter Russell argues for a concept of sovereignty that is capable of countering some of the colonial excesses of the past.[31] His starting point is the desire to understand Indigenous sovereignty claims as self-determination, juxtaposed against the claims to sovereignty that colonial powers have historically asserted over Indigenous peoples. According to Russell, sovereignty is a claim that is rooted in power: "The essential feature of the sovereignty claim is that those who make it for themselves or for the state they represent claim to be the highest source of legitimate power for the people and territory of their political community."[32] Russell emphasizes that rather than being an "incontestable fact,"

29. Note that Floridi argues for a need for new international sovereignty in the digital sphere, meaning greater international consensus over the governance of crucial aspects of digital society. Floridi, *supra* note 3.
30. Although conceding that multinational corporations wield considerable power, Chander and Sun counter the idea that corporations control the internet, offering examples of state pushback against perceived overreach. Chander & Sun, *supra* note 3.
31. RUSSELL, *supra* note 8.
32. *Id.* at 10.

sovereignty is a descriptor of a relationship.[33] He notes that the power historically wielded by the nation state is considerably more fragmented since the creation of the United Nations.[34] It is both challenged by, and sometimes shared with, entities that include international economic and trade institutions, global communications systems, and corporate technology giants.[35]

In emphasizing the nature of sovereignty as a claim, Russell suggests that it relies on two elements for its legitimacy. One is effectiveness: a claim of sovereignty will depend on how well the claimant is able to establish and maintain it.[36] This requires both internal and external support, as along with the potential for the use of force to support the claim.[37] The second dimension is legitimacy: a claim to sovereignty must have some moral or ethical basis, or it could be rejected or resisted.[38] In both of these senses, then, Russell describes sovereignty as a relationship (a) between sovereign states, and (b) between states and those that they seek to govern.[39]

III. MULTIPLE SOVEREIGNTIES

Although nation states are the principal locus of sovereignty in the traditional sense, the concept of sovereignty is capable of broader meaning. Sovereignty claims arise at a subnational level, particularly in federal states such as the United States and Canada, where legislative powers are divided between a national (federal) government on the one hand, and regional (state or provincial) governments on the other.[40] Although it is an issue not frequently discussed in the realm of technology policy, federalism, with its shared sovereignties, inevitably shapes the regulation of information technologies in federal states. This is in part because these technologies were unanticipated at the birth of many of today's federal states, and in part because their nature and impact cuts across the boundaries of those traditional categories that separate federal from state or

33. *Id.*
34. *Id.* at Chapter 8.
35. It is not that these entities are sovereign in the sense of nations. Rather, they exercise powers that may be delegated by the nation state (in the case of international organizations), administer international agreements between states, or act autonomously until curbed or curtailed by national laws (for example, in the case of corporations).
36. RUSSELL, *supra* note 8, at 10–11.
37. *Id.* at 10.
38. *Id.* at 11.
39. *Id.*
40. *See, e.g.* U.S. CONST. art. I; U.S. CONST. amend. X; Constitution Act, 1867, 30 & 31 Vict., c 3, ss. 91–92 (Can.).

provincial jurisdictions. AI itself involves systems that cut across all areas of endeavor. Although the structure and allocation of power within federal states can vary considerably, these levels of government are each sovereign with respect to their areas of legislative competence.[41]

Federalism can greatly affect national digital policy approaches. In data protection as well as in AI, much has been made of the U.S. approach to innovation as being one of "move fast and break things," and there is a considerable amount of ideology and industry lobbying that supports such an approach.[42] Yet at the same time, the United States has had to navigate the regulation of data and technology in a large and complex federal system in which not all normative evolution is meant to come from the central government. Indeed, recent and important developments in privacy law in the United States have come from the states, and a similar pattern may be emerging with respect to AI—or at least with respect to some AI-enabled technologies.[43] Canada too, as a federal state, has struggled to regulate some digital technology at the federal level.[44] For example, while the physical infrastructure of national transportation routes or telecommunications may fall easily and sensibly within federal jurisdiction, the governance of data or the regulation of AI—as a technology or as an industry—is less obviously a matter for federal rather than state or provincial jurisdiction.

What implications does federalism have for the regulation of AI? On one level, it may mean that regulation is slower and more decentralized, evidenced by

41. Ronald L. Watts, *Federalism, Federal Political Systems, and Federations*, 1 ANN. REV. POL. SCI. 117, 121 (1998).

42. *See, e.g.*, Cat Zakrzewski, *Tech Companies Spent Almost $70 Million Lobbying Washington in 2021 as Congress Sought to Rein in Their Power*, WASH. POST (Jan. 21, 2022), https://www.washingtonpost.com/technology/2022/01/21/tech-lobbying-in-washington [https://perma.cc/JKR3-5XXF]; Pawel Popiel, *The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power*, 11 COMMC'N CULTURE & CRITIQUE 566 (2018).

43. For an overview of developments in consumer privacy legislation at the state level in the US, see Pam Greenberg, *2022 Consumer Privacy Legislation*, NAT'L CONF. STATE LEGISLATURES (June 10, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx [https://perma.cc/UGB3-D3MD]. For U.S. state legislative initiatives relating to AI, see *Legislation Related to Artificial Intelligence*, NAT'L CONF. STATE LEGISLATURES (Aug. 26, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx [https://perma.cc/ LV3Q-YYUF].

44. The most notable example of this is private sector data protection. The current Canadian federal statute is grounded in the federal "general trade and commerce" power, but reliance on this power has constrained the scope of the bill. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.); *see also* TERESA SCASSA & MICHAEL DETURBIDE, ELECTRONIC COMMERCE AND INTERNET LAW IN CANADA, 109–12 (CCH Canadian Ltd. 2020).

the proliferation of state laws on privacy, biometrics, and facial recognition technologies in the United States. It is also possible for a federal government to play a coordinating and convening role. Such a role may necessarily be less coercive in nature than legislation.[45] Federalism may also favor ex-post regulation—at least initially—since jurisdiction over civil claims such as negligence or product liability will be well-established even if the authority to regulate a particular technology is not. Risk regulation, reaching across industries, sectors, and the life cycle of AI from design to deployment, is more challenging in a federal context where jurisdiction over some sectors and industries may lie with either federal or state or provincial governments.[46] Sectoral regulation may be easier, fitting established areas of legislative competence such as health, transportation, finance, and state and federal public sectors. Interestingly, what is often framed as an ideological set of choices may instead reflect pragmatism in the face of a political framework designed to share power across diverse sovereign jurisdictions.

Because federalism can make it difficult to move quickly and with one voice,[47] there is an argument for a convening and consensus-building role for a federal government in the digital sphere. Such a role is inherently consultative and multivocal. Russell argues that political structures that are genuinely federal offer "more freedom within the political communities with which we identify."[48] Federalism is in some ways more responsive to local culture and communities and to geographic, social, and economic differences.[49] As a result, the multiple sovereignties of federalism are important to consider in thinking about AI governance.

The concept of sovereignty is also importantly linked to self-government and decolonization.[50] Increasingly, sovereignty as self-determination has digital dimensions as well. For example, sovereignty is asserted by Indigenous peoples in

45. The AI Risk Management Framework from the National Institute of Standards and Technology is an example of a collaborative and consensus-based norm development process led at the federal government level in the US. NAT'L INST.OF STANDARDS AND TECH., AI RISK MANAGEMENT FRAMEWORK (2023).
46. Teresa Scassa, *Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act*, 101 CANADIAN BAR REV. (forthcoming 2023).
47. The exceptional nature of the EU's system in this regard is perhaps due to its explicit design to provide an overarching harmonized structure to accommodate distinct, preexisting sovereignties.
48. RUSSELL, *supra* note 8, at 85.
49. Watts, *supra* note 41, at 130–32.
50. *See, e.g.*, RUSSELL, *supra* note 8.

emerging and evolving Indigenous digital and data sovereignty movements.[51] In Canada, the First Nations Information Governance Centre (FNIGC)[52] has been a leader in defining and articulating Indigenous data sovereignty and in pressing national and provincial governments to recognize and support the Indigenous peoples' aspirations for this movement.[53] Indigenous claims to sovereignty over the digital and data processes and outputs by which a people is known, and thus governed, are at the heart of these movements.[54] Indeed, the Indigenous data sovereignty movement clearly delineates and exposes that data and their accompanying analytics and AI technologies are not neutral. There is power in choosing what data are collected, about whom, and for what purposes.[55] There is also power in choosing how they are to be analyzed and to meet what goals.[56] In this context, digital and data sovereignty are about much more than just where data are stored; they are about "the right of Indigenous peoples to govern the collection, ownership, and application of data about Indigenous communities, peoples, lands, and resources."[57] Indigenous approaches to AI which challenge the cultural context of AI development and governance are under development[58]

Another level of a sovereignty claim relates to the individual and speaks to the individual's ability to control aspects of the digital realm. Philosopher of technology Luciano Floridi defines digital sovereignty as a matter of control generally; translated to the individual level, he posits that "the ultimate form of control is individual sovereignty, understood as self-ownership, especially over

51. *See, e.g.*, Stephanie Carroll Rainie, Tahu Kukutai, Maggie Walter, Oscar Luis Figueroa-Rodriguez, Jennifer Walker & Per Axelsson, *Indigenous Data Sovereignty in* THE STATE OF OPEN DATA 300, 300–19 (Davies et al. ed., 2019); AUSTRALIAN NAT'L UNIV., INDIGENOUS DATA SOVEREIGNTY, (Tahu Kukutai & John Taylor ed., 2016).
52. FIRST NATIONS INFO. GOVERNANCE CTR., https://fnigc.ca [https://perma.cc/UZY7-W8GR].
53. *See, e.g.*, FIRST NATIONS INFO. GOVERNANCE CTR., OWNERSHIP, CONTROL, ACCESS AND POSSESSION (OCAP™) (2014).
54. INDIGENOUS DATA SOVEREIGNTY AND POLICY 2 (Maggie Walter, Tahu Kukutai, Stephanie Russo Carroll and Desi Rodriguez-Lonebear, eds., 2021).
55. *Id.*
56. *See* ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES AND THEIR CONSEQUENCES 19–20 (2014).
57. Rainie et al., *supra* note 51, at 301.
58. See, e.g., Indigenous Protocol and Artificial Intelligence Working Group, INDIGENOUS AI, https://www.indigenous-ai.net [https://perma.cc/8Q9B-VZLK]; INDIGENOUS PROTOCOL & A.I. WORKING GRP., INDIGENOUS PROTOCOL AND ARTIFICIAL INTELLIGENCE (Jason Edward Lewis ed., 2020); Karina Kesserwan, *How Can Indigenous Knowledge Shape Our View of AI?*, POL'Y OPTIONS POLITIQUES (Feb. 16, 2018), https://policyoptions.irpp.org/magazines/february-2018/how-can-indigenous-knowledge-shape-our-view-of-ai [https://perma.cc/E46B-Q3DD].

one's own body, choices, and data."[59] Although not equivalent to political sovereignty, discussed above, it is an evolving concept that has drawn from that sphere.

Elements of individual sovereignty have been appearing in data protection laws. From their inception, data protection laws have sought to balance the rights of the data subject with those of parties seeking to use that data—notably both governments and corporate actors.[60] The term data subject was coined to refer to the person to whom data related.[61] Data subjects hold rights under data protection law. Some of these rights were framed in terms of individual autonomy, most notably consent.[62] Yet the term data subject inherently suggests subjection. As the data economy evolved, this subjection became much more of a reality. Terms and conditions were dictated to users of technology who exercised little or no real control over the collection, use, or sharing of their data.[63] The EU's GDPR reflects a new generation of data protection law designed to give individuals greater control over their data through mechanisms that include data portability and rights of erasure.[64] For some, this is a welcome bolstering of individual sovereignty; for others, these changes do not go far enough in recognizing self-sovereignty with respect to data.[65] The changing role of the individual in data

59. Floridi, *supra* note 3, at 371.
60. The highly influential 1980 OECD "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" notes that "more extensive and innovative uses of personal data bring greater economic and social benefits", while at the same time emphasizing the importance of privacy protection. Org. for Econ. Coop. & Dev. [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, at 4, OECD/LEGAL/0188 (amended July 10, 2013).
61. For example, in the General Data Protection Regulation, *supra* note 10, at art. 4(1), a data subject is defined as "an identified or identifiable natural person."
62. Consent is an important feature of many data protection laws. *See, e.g.*, *id.* at art. 6(1)(a).
63. *See, e.g.*, ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA AND CORPORATE POWER (Cambridge Univ. Press 2021).
64. Versions of these rights can be found in legislation enacted or proposed elsewhere subsequent to the enactment of the GDPR. *See, e.g., California Consumer Privacy Act of 2018*, CAL. CIV. CODE § 1798.100–178.199.100 (West 2023); *Digital Charter Implementation Act*, *supra* note 26. Portability rights are also found in Singapore's Personal Data Protection Act 2020. No. 40 (Sing.).
65. Juan Caballero writes: Instead of a "right to be forgotten," which would be submitted as a request to the still-sovereign Data Controllers who might or might not honor such a request, we want subjects of data to get direct access to a "delete" button (or, to be more precise, a cryptographical "forget key" button). Instead of a promise to only share a subject's data in the ways originally agreed to, we want a form of data that cannot be shared in any other way, because the sovereignty of that subject is encoded in the 1s and 0s of the protocol by which the data itself is lent and transferred. Juan Caballero, *#SSI101: Self-Sovereignty and Autonomy*,

protection law has more recently led to individuals being described by some as the owners of their data, shifting the claim of sovereignty to the kind derived from ownership of a thing or resource, although this likely overstates the impact of these changes.[66] Nevertheless, the property paradigm evokes the right to exclude others as well as rights to control.[67]

Regardless of whether sovereignty is framed as control or ownership in this context, there is now a proliferation of normative frameworks and technological tools that aim to put the individual in control of their data.[68] Platforms such as Decode[69]—an experimental data governance platform that aims to facilitate control by individuals over their sensor data from connected devices—are designed, in their own words, to give individuals "ownership" of their personal data collected in the cities where they live, engaging individuals in decisions about data sharing.[70] In the private sector context, open banking systems, built upon the concept of data portability, are also described as models that give individual choices over how to share their data and with whom in order to serve their own needs.[71]

Greater personal control over data could impact AI as AI is inherently data-driven. For example, greater levels of individual control could shape access to data

MEDIUM (Oct. 28, 2019), https://medium.com/spherity/ssi101-self-sovereignty-and-autonomy-1874af797b4d [https://perma.cc/ 5F3H-YKUB].

66. For a discussion of the evolution of ownership claims in the United States, see Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. Rev. 423, 463–75 (2018); *see also* Teresa Scassa, *Data Ownership*, CTR. FOR INT'L GOVERNANCE INNOVATION [CIGI], No. 187 (Sept. 2018).

67. See, e.g., WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 12 (2003).

68. Professor Shoshana Zuboff writes of the failed idealism of an early smart home venture with localized data storage that the home owner would control, and how this vision was quickly supplanted by the data-extractive model she characterizes as typical of "surveillance capitalism." SHOSHANA ZUBOFF, *What Is Surveillance Capitalism*, *in* THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2020). The point here is that the individual control over data about themselves in the original model was framed in terms of "sovereignty" and reflected the ability to collect one's own data to use for purposes of one's choosing. *Id.*

69. DECODE, https://decodeproject.eu [https://perma.cc/ZRS7-LT9R].

70. *Id.*

71. *See, e.g.*, STANDING SENATE COMMITTEE ON BANKING, TRADE AND COM., OPEN BANKING: WHAT IT MEANS FOR YOU 8 (2019) (Can.) (describing open banking as "a framework to give customers more control over their financial data."); *see also* ADVISORY COMM. ON OPEN BANKING, FINAL REPORT 7 (2021) (Can.) (noting that open banking "provides consumers greater control over their data and enables them to securely use new data-driven financial services that can help them better manage their finances and improve their financial outcomes").

and place limits on its use.[72] Other emerging AI rights that are linked to data include the right to an explanation of automated decisionmaking. Some of the earliest legal provisions in relation to AI governance are found in data protection laws, including provisions that give individuals rights to challenge automated decisionmaking, to demand an explanation of it, or even to demand review of an automated decision by a human.[73] These provisions sketch out rights that, while not about individual sovereignty per se, carve out some space for individuals to exercise agency over how AI-enabled decisions are made about them. These rights reflect a notion of individual sovereignty that is akin to autonomy.

Yet the desire for greater individual control may be challenging to implement in the AI context. The right of erasure—another data protection right designed to enhance individual control over personal data—is a case in point.[74] Broadly speaking, such a right could allow individuals to withdraw their personal data from organizations and from those with whom the data have been shared.[75] In doing so, they can limit downstream uses of these data. In practice, the right of erasure may be difficult to realize effectively in a fast-paced AI innovation environment, in part because of the complex ways in which data are stored in systems.[76] Further, data protection laws tend to exclude from their scope anonymized personal data, limiting control over the use of personal data after it has been anonymized.[77]

Concerns over the use of data about humans—whether in identifiable form or not—are also taking normative shape. We see a growing number of claims

72. Critics of the EU's General Data Protection Regulation, for example, have argued that its protections will stifle innovation. *See, e.g.*, Scott Shackford, *Study: Europe's Aggressive Privacy Regulations Are Killing App Innovation*, REASON (May 10, 2022), https://reason.com/2022/05/10/study-europes-aggressive-privacy-regulations-are-killing-app-innovation [https://perma.cc/Q8RW-SS65].

73. *See, e.g.*, General Data Protection Regulation, *supra* note 10, at art. 22 (stating that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"); *California Consumer Privacy Act of 2018*, CAL. CIV. CODE § 1798.185 (West 2020) (providing for "[i]ssuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer"); Digital Charter Implementation Act, *supra* note 26, at § 63 (providing a right to an explanation of automated decision-making where such a system "could have a significant impact" on the individual).

74. *See, e.g.*, General Data Protection Regulation, *supra* note 10, at art. 17 ("[r]ight to erasure").

75. *Id.*

76. *See, e.g.*, Eduard Fosch Villaronga, Peter Kieseberg & Tiffany Li, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, 34 COMPUT. L. & SEC. REV. 304 (2018).

77. *See, e.g.*, General Data Protection Regulation, *supra* note 10, at Recital 26.

arising in relation to human-derived data.[78] These are data that are derived from humans and their activities but are not about identifiable individuals in a way that would bring these data under data protection law. Profiling uses data in this way, attributing certain characteristics to groups based upon inferences drawn from quantities of data. These are novel claims to group or collective privacy rights[79] that rely on a loosely (and often situationally) defined concept of sovereignty.[80] Some group privacy claims emphasize the power of AI to attribute correlations from group data to individuals and the potential for harm this might create.[81] Other claims are emerging in discussions about the use of population-level anonymized data. Such claims may involve assertions of the right to be consulted regarding the collection and use of the data. They may also involve access and benefit claims with respect to outputs.[82] For example, Ontario's report on the development of a health data ecosystem for that province provides that, "Health data must be governed to advance health and equity goals as determined and articulated through ongoing consultations with Ontario's people and communities."[83] In this context, the notion of sovereignty helps to "conceive of a group's right to control certain resources that are crucial to the collective interest of the group."[84]

CONCLUSION

The concept of sovereignty presents itself in different ways in the context of contemporary technology, including AI and the data that fuel it. More than just a new technology, AI takes on such economic importance that the race to set standards and develop governance for AI is seen as a central element in

78. *See generally* SPRINGER, GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Linnet Taylor, Luciano Floridi, & Bart van der Sloot, eds., 2016) (ebook).
79. For a broad discussion of the concept of group privacy, see *id.*
80. For example, in response to public concerns over the governance of human-derived data to be collected from a proposed smart cities project, the developer Sidewalk Labs proposed and defined the category of 'urban data' that would be subject to a form of collective governance. Teresa Scassa, *Designing Data Governance for Data Sharing: Lessons From Sidewalk Toronto*, TECH. & REGUL. 44, 44 (2020).
81. For example, a person's creditworthiness might be assessed based upon characteristics they share with a group rather than their own credit history. Lanah Kammourieh et al., *Group Privacy in the Age of Big Data, in* SPRINGER, *supra* note 79, at 37, 41–42.
82. *See, e.g.*, Scassa, *supra* note 80. The Ontario Health Data Council report on the development of a health data ecosystem in Ontario, Canada, takes particular note of group interests in health data, positing that uses of health data should respect "the dignity and integrity of people, groups, and communities." ONT. HEALTH DATA COUNCIL, ONTARIO HEALTH DATA COUNCIL REPORT: A VISION FOR ONTARIO'S HEALTH DATA ECOSYSTEM, 23 (2022).
83. *Id.* at § 4.3.
84. Kammourieh et al., *supra* note 81, at 55.

establishing nations' future or ongoing place in the global power hierarchy. Powerful, data-driven, inscrutable, and increasingly difficult-to-challenge automated processes and decisionmaking will impact individual and collective sovereignties.

What can we learn from the way in which the concept of sovereignty presents itself in the AI and data context? First, that we are in the midst of a societal and economic shift which is disrupting existing power structures and frameworks. Second, although digital sovereignty is a concern at the national and international level, conversations about digital, data, and AI governance are taking place at multiple levels. Unsurprisingly, this includes international organizations, but it also includes subnational governments, such as self-determining communities and communities of shared interest. Third, sovereignty has always had some application as a descriptor of the relationships between national and subnational governments and has relevance in self-determination movements. Yet the growing use of a concept of sovereignty in relation to communities, and even individuals, reveals emerging normative claims to rights to participate in digital governance below the governmental level. Technology expands risks and challenges, but it also provides tools that can facilitate more direct engagement and choice, as well as more situational and localized governance.