weizenbaum journal OF THE DIGITAL SOCIETY

03 ISSUE 02

WEIZENBAUM JOURNAL OF THE DIGITAL SOCIETY
Volume 3 \ Issue 2 \ w3.2.7 \ 11-08-2023
ISSN 2748-5625 \ DOI 10.34669/WI.WJDS/3.2.7

Information on this journal and its funding can be found on its website:
https://wjds.weizenbaum-institut.de

KEYWORDS

digital sovereignty
data colonialism
migration
racism
smart borders

VOICES FOR THE NETWORKED SOCIETY

Sovereignty and Its Outsiders

Data Sovereignty, Racism, and Immigration Control

Ulises A. Mejias

State University of New York at Oswego
ulises.mejias@oswego.edu

ABSTRACT

The concept of sovereignty invokes a nation's authority, autonomy, and power to act. Recent societal developments invite new questions about that concept. For example, on whose behalf is sovereignty declared, particularly when it comes to "data sovereignty"? How are the benefits and costs of data sovereignty distributed in a society? Data sovereignty signals that the data produced within a certain territory should be bound by the laws and rules of that territory. However, this article argues that people on the move (migrants, refugees, and asylum seekers) are excluded from claims to data sovereignty and treated as objects of datafied persecution. That is, they are outsiders to sovereign spaces, both geographic and datafied. To investigate this situation, this article explores the historical echoes of the term "sovereignty," especially given that the concept was particularly invoked in colonial times as a nation-building tool, applied when colonies claimed their independence while at the same time establishing internal social hierarchies. This analysis suggests that race continues to represent a key element in the hi-tech exercise of sovereignty at the border, replicating colonial and extractivist injustices against groups that are increasingly vulnerable in contemporary societies.

1 Introduction

The rise of the internet as a global information and communication technology has been accompanied by the assumption that national borders – and, by extension, national sovereignty – have become increasingly unimportant. That is, if information can travel across geopolitical boundaries and facilitate collaboration between individuals and communities, surely geopolitical lines should no longer represent effective instruments of control. However, sovereignty has made a discursive return. States and communities are grappling with a world order that sees a handful of corporations control the means of data collection, circulation, and processing, including the transformation of public data into training data for artificial intelligence models. In this context, sovereignty has emerged as a manifestation of a desire for autonomy and self-determination in opposition to the interests of dominant tech companies.

The concept of sovereignty invokes a nation's authority, autonomy, and power to act. However, pertinent claims persist around that concept, especially given recent technological developments. For example, on whose behalf is sovereignty declared? That is, who is included and excluded from claims to sovereignty? Are the benefits and costs of sovereignty and claims to sovereignty justly distributed in a society?

Here, I aim to situate notions of data sovereignty within the context of the assertions of authority and autonomy that they represent and to ask at whose expense these claims are made. I am choosing to focus on "data sovereignty" here, even though the term is sometimes used interchangeably with "digital sovereignty" (the latter could be said to be a more extensive category focusing on technological infrastructures, while the former more specifically concerns the digital information generated by those infrastructures).

What interests me in particular are the historical echoes of the term "sovereignty" itself. The concept was invoked in colonial times as a nation-building tool, applied when colonies claimed their independence. Therefore, I am concerned with how the term resonates in contemporary discourses about who is considered inside and outside of the sovereign "data territory" (Mejias & Couldry, in press). As nations grapple with issues of data sovereignty, "people on the move" (migrants, refugees, and asylum seekers) have emerged as the object of datafied persecution, outsiders to sovereign spaces. This dynamic primarily intends to enable wealthy nations to externalize their borders, blocking such outsiders from reaching those nations while generating enormous profits for the corporations that develop surveillance and border control tools. Many of the examples mentioned here relate to Latin America. But given the replication of similar dynamics elsewhere, the implications are obviously global.

2 Data Sovereignty and Big Tech

At a basic level, data sovereignty can be interpreted to signal that data produced within a certain territory should be bound by the laws and rules of that territory. Sidestepping isolationism, scholars have attempted to associate data sovereignty with values such as international coordination, solidarity, and human rights (Couture & Toupin, 2019; Becerra & Waisbord, 2021; Gilwald & Murdick, 2022).

However, this vision presents many challenges and obstacles. First, the sheer political power that Big Tech corporations have acquired allows them to directly confront states when their interests are threatened (recall, for instance, how Facebook imposed a news blackout in Australia in 2021 in response to attempts by the government to tax its use of content). Another challenge is the nature of multinational trade deals, particularly those involving Global South nations doing business with either the US or China. These treaties often block data sovereignty efforts by prohibiting data-localization measures (i.e., the ability of a nation to demand that data generated by its citizens is stored within its borders), engaging in stringent protection of intellectual property, or forcing governments to endorse foreign laws, such as Section 230 of the US Communication Decency Act, which guarantees immunity to US companies with respect to the content uploaded to their platforms by users (Haggart, 2018; Becerra & Waisbord, 2021).

In this context, we see states increasingly try to claim independence from Big Tech, by which I refer to not only US-based companies (e.g., Alphabet, Apple, Amazon, Meta, Microsoft, Palantir) but also the corporations controlled by the Chinese Communist Party, including Baidu, Alibaba, Tencent, and Xiaomi.

Perhaps the clearest example of this resistance is the European Union (EU), which has struggled to find its own strategic autonomy in a post-Brexit world that includes a war on Europe's eastern frontier. Laws such as the General Data Protection Regulation (GDPR) and the proposed AI Act serve as important markers of sovereignty simply by attempting to regulate an industry that remains largely unregulated in most parts of the world. The 2020 EU Court of Justice "Shrems II" ruling, which requires European companies to assess each data transaction with non-EU countries, is also designed to send a strong message to the locus of Big Tech in Silicon Valley.

However, Global South nations have less bargaining power with which to confront the status quo. For instance, Latin America has adopted a decisively non-nationalistic approach to its data, choosing instead a laissez-faire regulatory approach that does not challenge what the US government and Silicon Valley prescribe. This is unsurprising given the relatively small size of Latin America's digital economies. Nonetheless, at the same time, Latin America has welcomed investments from China in its data sector, once again placing the region at the intersection of the interests of two superpowers, especially in the context of the race to dominate AI.

This does not mean Latin America completely lacks data sovereignty proposals. Many countries in the region have enacted laws resembling Brazil's General Personal Data Protection Law and those laws instituted by Mexico's National Institute of Transparency, Access to Information, and Protection of Personal Data (which governs the processing of data by foreign companies). However, data sovereignty must be understood in an older historical context, a context that is unfortunately tainted by racism.

3 Colonial Roots of Sovereignty

As "New World" colonies claimed independence from European powers, they used the concept of sovereignty as a tool for building independent nations. But as Maldonado-Torres argues (2015, pp. 69–71), the models of sovereignty that emerged from this process were based on different and often contradictory ontologies, at least in the American context. Given that race represented a primary axis in the matrix of colonial power, its central role in these models is to be expected, shaping an implicit hierarchy of different kinds of racially informed sovereignties which rendered some types of independence more viable and acceptable than others.

At the top of this hierarchy was the sovereignty of the United States from England in the 18th century. This struggle for independence was accepted in international relations as viable and conceptually possible or thinkable because it involved white men claiming independence from other white men. Certain assumptions about the racial order of the world were left untouched, including slavery.

Haitian independence represented the other end of the spectrum. The declaration of sovereignty by black slaves from white masters was seen in international relations terms as an unthinkable and illegitimate expression of sovereignty, a threat to the status quo (likely the reason that the US refused to recognize Haiti as a sovereign nation until 1862).

Between these two extremes, the struggle for sovereignty in Latin America in the early 19th century developed as a *partly* thinkable project because it was undertaken by mixed-race individuals (mestizos). The revolting elites of these countries, which had strong roots in Europe, were able to frame their fight for independence in terms that made sense to the Western world while selectively including some elements of indigenous culture (elements not considered threatening). In essence, although sovereignty in Latin America invoked a discourse on liberty, that iteration of liberty reflected a clear racist hierarchy that situated indigenous people and black slaves at the bottom.

I believe that these historical lessons can contribute to our interpretation of the development of data sovereignty. Accounts of the independence movements that swept the American continent can help us understand how, centuries later, data sovereignty projects emerge as thinkable or unthinkable in relation to defining who is inside and outside the sovereign nation. Although data can flow freely across borders, those borders are often closed to certain groups of people, and digital technologies (including data) are used to control and even block their movement. Race continues to be a key element in this hi-tech exercise of sovereignty at the border, replicating colonial and extractivist injustices against a group that is increasingly vulnerable in our societies: non-white migrants.

4 Migrants at the Smart Border

Undeniably, we are experiencing a global migration crisis. The United Nations High Commissioner for Refugees indicates that there were 108 million forcibly displaced people in 2022, 76 percent of whom were hosted by low- and middle-income transit countries. Of course, the migration crisis is intertwined with other problems including global warming, war, poverty, and political instability.

In the last three decades, border externalization has been a primary strategy for attempting to control the flow of people from Africa and the Middle East into Europe and from South and Central America into North America. Data captured using surveillance technologies is an important tool in this process, particularly because the tracking of migrants can be used as a bargaining chip by origin and transit countries to secure more funding from wealthy nations trying to curb migration through border externalization (Napolitano, 2023).

Border security is a highly profitable sector worth US$45.9 billion as of 2022 and projected to reach US$70.5 billion by 2030 (Border Security Systems: Global Strategic Business Report, 2023). In the US, some of the companies with government contracts related to border security include Amazon, Clearview, Dell, Hewlett-Packard, LexisNexis, Microsoft, Palantir, Salesforce, and Thompson Reuters (Lackowski et al., 2021; Mijente et al., 2018). In Europe, the border control agency Frontex has the largest budget of all EU agencies, and its ties to military and security companies are on the rise (Akkerman, 2023). This political and economic reality promotes a view of migrants and refugees as “data points” to be used as a source of revenue and a means to exert political pressure, with data extraction key to both applications.

Data is responsible for the near ubiquity of the Smart border. That the surveillance technologies behind Smart borders are often exploitative, biased, and even based on unscientific premises is not stopping corporations or states from deploying them within and beyond borders. These technologies help to profile, assess, detain, prosecute, and punish migrants, with AI models increasingly employed to "predict" events or outcomes before they even happen (Napolitano, 2023). For example, the EUMigraTool project (https://www.itflows.eu/eumigratool) uses AI to predict migrant flows and monitor antagonistic attitudes in destination countries (although the project has good intentions and claims to strive towards humanitarian goals, it is an example of how migration can be framed as a problem that can be explained and managed through data and AI).

Indeed, even before crossing a border, migrants are exposed to an arsenal of extractive technologies through financial tracking, interactions with automated AI agents who review cases and applications (Rud, 2023), the implementation of risk assessment and knowledge management tools by border agents, and the increasingly sophisticated use of aerial, water surface, underwater, and ground unmanned drones (the EU's ROBORDER project is an example of this). At the border, migrants might encounter all sorts of biometric capture systems, AI lie detection systems, remote and mobile video surveillance and facial recognition (capable of identifying individuals six miles away, day or night), automated license plate recognition, and mobile phone confiscation and analysis. After crossing the border, asylum seekers might be subjected to continuous monitoring through technologies like ankle bracelets, which can also record sound and which, in the US, refugees must pay for themselves. Non-citizens are then subjected to the kind of tracking that citizens are also subjected to, which includes monitoring using data from government agencies, public services, and social media. All these systems are increasingly interconnected by powerful data analytics tools such as Palantir's Investigative Case Management system, which can produce data "insights" built on sophisticated database integration, pattern recognition and visualization tools. Because corporations can claim trade secrecy, and governments can claim state secrecy, there is no accountability, transparency, or opportunity to track abuses that the application of these technologies might produce (Mijente et al., 2021).

Irregular migrants (those without documents) are at greater risk. First, as more and more steps of the residency or refugee application process move online, this low-income population is least likely to be able to access the necessary digital platforms to submit their paperwork, as a UN report about migrant human rights noted (Gonzales Morales, 2023). Second, this population might be more easily compelled to submit to biometric data extraction in the belief that it might help their case. Although countries such as Colombia and Chile engage in this kind of biometric collection (not to mention China and the US), there is no transparency about how the data is used (Camacho, 2023).

It is also worth noting that the datafication of the border is welcomed by parties across the political spectrum, with liberals seeing it as a form of techno-humanitarianism that helps to deter migrants in an effort to avoid disastrous outcomes, and conservatives considering it a form of techno-policing that keeps undesired migrants and presumed terrorists away. Both liberal and conservative views of Smart borders are lethal because they both precipitate expansions of areas under surveillance. This forces migrants to attempt to cross borders under more dangerous conditions, resulting in increased loss of life (Chambers et al., 2019).

What does all of this have to do with sovereignty? If sovereignty describes an attempt to legitimize authority over a territory by defining that territory's borders, articulating sovereignty requires defining who is included and excluded from that territory. When it comes to data practices, migrants and refugees are seemingly outside of sovereign space, and states and corporations can engage in predatory and extractivist practices with few repercussions. Even supposedly progressive legislation, such as the EU's AI Act, has failed to specify measures to protect the rights of migrants against invasive and discriminatory systems, effectively creating "a two-tiered AI regulation, with migrants receiving lesser protections than the rest of society" (Napolitano, 2023, p. 14). Progressive groups in civil society (e.g., https://protectnotsurveil.eu/) demand that governments and international bodies put protective measures in place as soon as possible. Strict controls should also be enforced on corporations profiting from this form of surveillance. Of course, protecting migrants against datafied persecution will not solve the global migration crisis. However, it is an important step in the struggle for human dignity. Without attempts to protect migrants from exploitation by extractivist data practices, data sovereignty will remain an empty concept that simply replicates old injustices.

In memoriam Patricia R. Zimmermann, friend and mentor.

References

Akkerman, M. (2023, May 31). *Global spending on immigration enforcement is higher than ever and rising*. Migration Policy Institute. https://www.migrationpolicy.org/article/immigration-enforcement-spending-rising

Becerra, M., & Waisbord, S. R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public*, 6(1–4), 67–79. https://doi.org/10.1177/20570473211046730

Border Security Systems: Global Strategic Business Report. (2023). Global Industry Analysts, Inc. https://www.researchandmarkets.com/report/border-security#tag-pos-4

Bosoer, L. (2022, October 26). *Digital sovereignty: Voices from Latin America*. Latin American Focus Group. https://blogs.eui.eu/latin-american-working-group/digital-sovereignty-voices-from-latin-america/

Camacho, L. (2023, August 11). *Migrantes sin papeles y su regularización* [Undocumented migrants and their regularization]. Derechos Digitales. https://www.derechosdigitales.org/22163/migrantes-sin-papeles-y-su-regularizacion/

Chambers, S., Boyce, G., Launius, S., & Dinsmore, A. (2019). Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico Border: A geospatial modeling of the geography of deterrence. *Journal of Borderlands Studies*, 36, 1–26. https://doi.org/10.1080/08865655.2019.1570861

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Gilwald, A., & Murdick, D. (2022). *Data justice policy brief: Putting data justice into practice*. Global Partnership on Artificial Intelligence.

González Morales, F. (2023). *Report on how to expand and diversify regularization mechanisms and programs to enhance the protection of the human rights of migrants*. United Nations Office of the High Commissioner for Human Rights. https://www.ohchr.org/en/calls-for-input/2023/report-how-expand-and-diversify-regularization-mechanisms-and-programs-enhance

Haggart, B. (2018, October 28). *Make no mistake: The USMCA is an America-first trade deal*. The Conversation. http://theconversation.com/make-no-mistake-the-usmca-is-an-america-first-trade-deal-104818

Lackowski, A., Salgado, R., & Freier, M. (2021). *Sabotaging sanctuary: How data brokers give ICE backdoor access to Colorado's data and jails*. Mijente, Colorado College Summer Immigration Institute and the Colorado Immigrant Rights Coalition. https://coloradoimmigrant.org/wp-content/uploads/2022/04/Sabotaging-Sanctuary_Final-Report_Design-4-1.pdf

Maldonado-Torres, N. (2015). Colonialism, neocolonial, internal colonialism, the postcolonial, coloniality, and decoloniality. In Y. M.-S. Miguel, B. Sifuentes-Jáuregui, & M. Belausteguigoitia (Eds.), *Critical terms in Caribbean and Latin American thought: Historical and institutional trajectories* (1st ed., pp. 67–78). Palgrave Macmillan.

Mejias, U. A., & Couldry, N. (2024). *Data grab: The new colonialism of Big Tech and how to fight back*. WH Allen.

Mijente, Just Futures Law, & No Border Wall Coalition (2021). *The Deadly Digital Border Wall*. https://notechforice.com/wp-content/uploads/2021/10/Deadly.Digital.Border.Wall_.pdf

Mijente, National Immigration Project, & Surveillance Resistance Lab (2018). *Who's behind ICE? The tech and data companies fueling deportations*. https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

Morrison, S. (2023, June 16). *The US government is buying your data to spy on you*. Vox. https://www.vox.com/technology/2023/6/16/23762403/data-odni-report-wyden

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

Napolitano, A. (2023). Artificial intelligence: *The new frontier of the EU's border externalisation strategy*. EuroMed Rights. https://euromedrights.org/wp-content/uploads/2023/07/Euromed_AI-Migration-Report_EN-1.pdf

Rud, J. A. (2023, June 20). Asylum text analytics as an algorithmic silver bullet: The impossible quest for automated fraud detection. *Talking Politics*. https://talkingpoliticsonline.blogspot.com/2023/06/asylum-text-analytics-as-algorithmic.html?m=1