G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

TF05

Policy Brief

Private Algorithms and Public Interest

Overhauling the Trade Secrets Regime for Equitable AI Futures

IT for Change

DataPrivacyBR

Private Algorithms and Public Interest:

Overhauling the Trade Secrets Regime for Equitable AI Futures

Taskforce 5.5. Challenges, Opportunities, and Governance of Artificial Intelligence

Authors:

Anita Gurumurthy, Executive Director, IT for Change (India)

Shreeja Sen, Research Associate, IT for Change (India)

Mariana Rielli, Co-director, Data Privacy Brasil (Brazil)

Table of Contents

Private Algorithms and Public Interest:

Overhauling the Trade Secrets Regime for Equitable AI Futures

Abstract

The use of trade secrets to enclose the data undergirding artificial intelligence (AI) systems is a dimension that remains under-explored. This policy brief posits that the data enclosed in trade secrets by digital transnational corporations has the effect of stifling genuine innovation and makes AI systems non-transparent and unexplainable. While trade secret regimes are important for the functioning of innovative markets, they have tended to extend outwards and cover an increasing number of information goods of the nature of data in both commercial and non-commercial contexts. For instance, trade secret claims in the information-feeding recidivism algorithms have been used to deny requests by incarcerated individuals to understand why they were given a particular rating. The increasing prominence of AI in economic and social life compels an examination of the extent to which AI-related innovations should be protected under trade secret provisions.

Trade secret protections are increasingly used to evade data or algorithm-sharing mandates in lieu of intellectual property (IP) protections where the latter are deliberately kept sparse for public welfare objectives. This policy brief examines the different impacts of trade secret regimes in the data and AI paradigm and offers forward-looking recommendations to ensure that trade secret protections do not end up creating monopolistic control over data, and that there is a transparent, inclusive, equitable, and accountable AI system.

Keywords

AI systems, data, trade secrets, intellectual property, digital transnational corporations

I. Diagnosis of the Issue

The start of the millennium was about the unprecedented promise of a new knowledge paradigm. The internet as the global commons was heralded as the force that would democratize knowledge production. The advent of the platform, and with it, the potent resource of Big Data, was yet another turning point. Here was a non-rivalrous resource that could be used endlessly to build insights for the advancement of humanity. Yet, AI, the leitmotif of the data revolution, is the very antithesis of the original digital promise. AI systems and models, built on top of a finders-keepers logic of first-mover platform companies have restructured the datasphere. Large firms in the digital marketplace have proprietized the intelligence derived from data, while rendering the data they have collected and hoarded inaccessible.

Intellectual property (IP) rights are often cast as the bulwark on which innovation takes place—they offer exclusive rights in exchange for purported continued development and progress. While research shows that this is not necessarily the case (Brüggemann 2015), corporations continue to push for IP protection through patents, copyrights, and trade secrets. IP rights also become a form of public policy (Kilic 2024): a measure to balance recognition of innovation (and rights holders) with the public interest (in the creation and sustenance of the knowledge commons). For the purpose of this policy brief, the focus will be on trade secrets, as a less prominent issue that needs to be tackled in relation to data and AI systems.

Trade secrets are unique in their conception since, unlike patents or copyrights, they do not come with a limited time protection. In the case of AI systems, the undergirding data is treated as secret. The three key requirements for the grant of trade secret protection—also captured in the TRIPs agreement, the EU Trade Secrets Directive, and the US Uniform Trade Secrets Act—are: the information sought to be protected must be secret and not easily available to experts in the field; there must be commercial or economic value in keeping the information secret; and there must have been reasonable steps taken to keep this information secret. Trade secrets in the digital economy are increasingly becoming the go-to system of protection since data is not patentable and has limited copyright coverage (Radauer, Searle and Bader 2023). The consequence is that large amounts of aggregate data collected by Big Tech (including firms like Amazon and Google that have major stakes in multiple domains as well as sector-specific lead firms like Uber, Deliveroo, etc.) from transaction activity of users and from public datasets also becomes proprietized (Segal 2024).

The accessibility of aggregate data, whether processed or not, is a core element for any data governance regime. However, IP rules often lead to restriction of data sharing mechanisms. For instance, the EU Data Act, intended to enable third-party data sharing from smart devices, provides for exceptions to trade secret holders to withhold information sharing in certain circumstances (Mylly

2024). Trade secrets protection of data has two serious consequences: maldistribution (unfair distribution of access and benefits) and misrecognition (identity-based exclusion and harm) in the data economy:

- The social data commons is enclosed because a few firms retain exclusive ownership of data. The fragmented enclosures result in the "tragedy of the anticommons," which refers to the wasteful underuse of the given resource (Heller 2013). Trade secrets in data disincentivize innovation, preventing the non-exclusive access necessary for exploring data's multifarious propositions and the right of all economic actors to meaningfully leverage data for unlocking its value.
- Trade secrets in data also render AI systems built on the data unexplainable. This is seen in recidivism tracking algorithms, as in the US case of *Loomis v. Wisconsin*. The defendant, Eric Loomis, was sentenced to six years imprisonment because of his rating on a recidivism predictor algorithm and subsequently denied the right to access information on the algorithm to understand why he received this rating since this information was considered a trade secret by the developer (Moore 2017).

To incentivize the optimal use of data for socially relevant AI innovation and to uphold the human rights of those implicated by the AI, data governance regimes must preserve the openness of data, promoting its discoverability, accessibility, sharing, and reuse, while ensuring scrutinizability to prevent harms and protect rights.

II. Recommendations

Through the following recommendations for reforming the trade secrets regime in data that run AI systems, the G20 can ensure that the data and AI paradigm can be just and equitable. Specific action items are included in the recommendations.

1. Introducing a proposal for a global governance framework for data.

The G20 should initiate a proposal to introduce a global governance framework for data at the UN level that ensures economic justice and enables a global knowledge democracy. Monopolies built on the misuse of trade secrets have entrenched themselves in the market, locking up data's immense potential for the sustainable development goals (SDGs). The global governance framework must straddle the imperative for accessibility of data and nurturance of the data commons as humanity's collective heritage, and the need to ensure transparency and explainability of systems built on such data. There have been recommendations made to ensure legislations, like the EU Data Act, enable the sharing of both inferred and derived data, as well as aggregated datasets from multiple users to ensure

that such data-sharing provisions are successful (Radauer et al. 2022). In fact, differentiated sharing regimes—which require states, private corporations, and other actors to access and share data in specific ways—can ensure there is no enclosure of public data/insights from public data, and private data is available for states to perform their public functions in the public interest (Gurumurthy and Chami 2022).

2. Recalibrating the IP regime for an equitable, inclusive, and accountable AI paradigm.

For the AI paradigm to be equitable, inclusive, and accountable, governance mechanisms need to cater to the needs of Global South nations. The Covid-19 pandemic was proof that IP regimes don't address social justice considerations without explicit mandates (Thambisetty 2022).

Encouragingly, a recent resolution adopted by the UN General Assembly underscores the need for safe, secure, and trustworthy AI, noting the need to promote "transparent, inclusive, and equitable use of AI while respecting intellectual property rights and privacy" (U.S. Department of State 2024). This resolution checks all the right boxes with regard to human rights considerations in AI, privacy rights, and building governance mechanisms for AI, but it needs to go the distance with regard to a legally binding accountability and liability mechanism for companies as well as states. Big Tech, in particular, is infamous for evading compliance on many counts in jurisdictions across the world (Browne 2024; Ocampo, 2019). Lead firms have also refused to share data with local governments, and calls for voluntary data sharing have met with limited success (Adenubi 2024). Even common data spaces envisaged in the EU have failed to create avenues for the pooling of voluntary data (Scerri et al. 2022). In that regard, transparency, inclusivity, and equity in the use of AI require much more than an emphasis on risk and impact assessments that the recent UN resolution recommends. It needs a deeper interrogation of the manner in which trade secrets protection stands in contrast to and prevents the realization of ideals articulated by the resolution.

Additionally, while intellectual property regimes were created to give due credit to creators and innovators, to support genuine innovation and enable the democratization of knowledge, this goal has been subverted to the profit motives of large transnational corporations (Hanna, Brown and Brette 2020). While it is accepted that raw data does not have trade secrets protection (Mylly 2024), it is often used as a veil to assert market power, circumvent requirements of transparency, inclusivity, and accessibility, and block innovation. This contradiction, which forms the current political economy of AI, stands in the way of justice and development in today's global digital economy.

In essence, Global South countries face dual challenges: loss of control over access to data, especially at the domestic level because regulating transnational corporations can be difficult; as well as the

inability to scrutinize algorithms that impact national-level welfare policies like health, education, financial support, and citizens' human rights. To grapple effectively with the huge inequalities in the AI economy, and bring to bear an indivisible and integrated approach to human rights in AI, a radical stock-taking and reform of the IP regime is in order internationally.

Trade secrets protection of data in AI systems has far-reaching consequences for an equitable, inclusive, and accountable AI paradigm. The governance of AI systems must not be decoupled from the wicked problem of data enclosures and data colonization (Gurumurthy and Chami 2019). G20 members can galvanize around the issue of misuse of trade secrets protection in the digital economy, using upcoming UN processes—the Global Digital Compact and the 20th-year review of the World Summit for Information Society—to address the role of IP in promoting a genuine dynamic of innovation in the AI economy.

3. Checking the overexpansion of the IP regime for a just data and AI paradigm.

IPR, in particular, trade secrets protections, must not be used to restrict data accessibility and transparency of AI systems. As such, the IP regime should be limited to existing types, like patents, copyrights, etc., and must not be expanded judicially. National courts and parliaments are crucial authorities who can ensure overexpansion of trade secrets in non-personal or aggregate data is stymied, as well as balance the rights of non-owners of data. Such restriction and balancing through access to aggregate data can be on the grounds of freedom of information, freedom of scientific research, and freedom of free movement of data to enable the provision of welfare services (Fia 2022). For instance, the European Court of Justice's statement that companies cannot argue non-disclosure of their algorithms because of IP or trade secrets considerations to explain AI systems within the scope of Article 22 of GDPR is an important step towards eliminating the reliance on trade secrets to restrict data access, except for very few considerations identified by the court, such as national security and criminal matters (Stankovich 2024, 110).

4. Modifying the scope of antitrust norms to examine trade secrets provisions.

It is imperative to study the impact of trade secrets provisions from an antitrust perspective, to understand whether such protection is sought to preserve and retain dominant status in markets (Portuese 2018). Trade secrets provisions are often considered part of unfair competition rules, rather than intellectual property, and it is important that national regulatory authorities scrutinize their role in restricting competition. G20 members can initiate a systematic study into this to create an evidence-based resource for next steps so that national regulators are able to operationalize adequate measures to keep their markets competitive.

III. Scenario of Outcomes

The following scenarios of outcomes can be envisaged if trade secrets in data are restricted.

1. Pushback from platform companies.

The technology industry has been pushing back against calls for greater transparency and explainability of AI systems and demands to disclose trade secrets on the ground that such regulatory demands will stifle innovation (Bloch-Wehba 2021). The recommendations proposed in this policy brief will restrain technology companies' claim to trade secrets over their data in AI systems and will require them to be transparent about their source code and datasets used. This is likely to be resisted by the industry. This resistance must be weighed against the enormous public benefits of making AI systems equitable, inclusive, transparent, accountable, and explainable in terms of ensuring economic and social justice and safeguarding the knowledge commons. Moreover, studies have shown that IP protections, including trade secrets, in fact, restrict innovation in the long run due to restricted knowledge flows and reliance on self-produced prior innovation rather than the best innovation available, and consequent decrease in welfare (Intellectual Property Office 2021).

2. Potential exit of Big Tech services or withdrawal of services from countries implementing data-sharing rules.

Big Tech companies are known to use the threat to leave jurisdictions, or actually leave jurisdictions, or limit their services when regulations are imposed that do not favor them (Matza 2023). However, it is possible that other companies can grow in the absence of Big Tech's dominance to provide better services provided public policies create a robust innovation ecosystem.

3. Accessible data for public innovation and competitive markets.

A positive outcome of ensuring that trade secrets are not misused to enclose data is that this data will be available for true public innovation by smaller companies for whom Big Tech's massive intelligence advantage acts as a barrier to entry. This would also create scope for competitive markets, allowing local innovations to displace Big Tech monopoly and give impetus to a wider public and private innovation.

4. Domestic policy change for appropriate public policies and right to development.

States can draw insights from large aggregate data collected by tech companies based on non-negotiable principles of a global data constitutionalism and through national data governance frameworks that prevent abuse of IP rights and encourage a balanced approach to public innovation. It is imperative for a just AI economy, both at the national and global levels, to enable AI transparency

through the ability to scrutinize the underlying data held by digital transnational corporations. In fact, a big win for the Lagos government is the ride-hailing company Uber agreeing to share trip data after initially refusing to do so (Megawai 2024).

5. The role of free trade agreements in undermining fair data practices.

Domestic policy reforms to mandate transparency of AI systems and reforming the trade secret protection available to AI systems may be circumvented by bilateral or plurilateral trade rules that contain provisions that bar governments from requiring companies to disclose source code and datasets used (Ruggeroni 2023). This limits the policy space of national governments to regulate AI systems deployed in their jurisdiction to ensure that human rights are upheld, economic justice is not undermined, and harms to society are reduced. Trade agreements, which are not democratically debated and heavily prone to lobbying by Big Tech companies (Data Privacy Brasil 2023), should not be allowed to impinge on domestic regulatory efforts, particularly in Global South countries, to usher in a just, fair, and equitable AI paradigm in their jurisdiction.

If G20 members can rally support for equitable and just AI systems, it may lead to the renegotiation of certain trade rules, especially on restriction of source code disclosure. The free digital trade agenda currently reinforces asymmetries at all levels, including in terms of countries' abilities to gain maturity in their technological development, and protect and promote the rights of citizens. A transformation of the IP regime to democratize data access and data value will be a big win for a democratic and equitable digital transformation, endorsing Brazil's G20 priority of reforming global governance institutions.

Bibliography

- Adenubi, Tola. 2024. “Uber, Lagos govt on collision course over data sharing agreement.” Zawya. https://www.zawya.com/en/world/africa/uber-lagos-govt-on-collision-course-over-data-sharing-agreement-iiq8cgph
- Bloch-Wehba, Hannah. 2024. “Transparency’s AI problem.” Knight First Amendment Institute at Columbia University. https://knightcolumbia.org/content/transparencys-ai-problem
- Browne, Ryan. 2024. “Amazon, Microsoft, Meta and others accused by rivals of not respecting new EU competition rules.” CNBC. https://www.cnbc.com/2024/01/16/24-companies-sign-open-letter-saying-big-tech-isnt-respecting-eu-dma.html
- Brüggemann, Julia et al. 2015. “Intellectual property rights hinder sequential innovation - Experimental evidence.” CEGE. https://www.econstor.eu/bitstream/10419/106128/1/814347134.pdf
- Data Privacy Brasil. 2023. “The intersection between AI regulation in the South and digital trade clauses involving source code and algorithms.” https://www.dataprivacybr.org/en/the-intersection-between-ai-regulation-in-the-south-and-digital-trade-clauses-involving-source-code-and-algorithms/
- Fia, Tommaso. 2022. “Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data.” *International Review of Intellectual Property and Competition Law*, Volume 53 (June). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123311
- Gurumurthy, Anita and Nandini Chami. 2022. “Governing the Resource of Data: To What End and for Whom? Conceptual Building Blocks of a Semi-Commons Approach.” IT for Change. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4037323
- Gurumurthy, Anita and Nandini Chami. 2019. “The Wicked Problem of AI Governance.” Friedrich Ebert Stiftung and IT for Change. https://itforchange.net/sites/default/files/1625/The%20Wicked%20Problem%20ofAI%20Governance.pdf
- Hanna, Thomas, Dana Brown and Miriam Brett. 2020. “Democratizing knowledge: Transforming intellectual property and research and development.” The Next System. https://thenextsystem.org/democratizing-knowledge
- Heller, Michael. 2013. “The Tragedy of the Anticommons: A Concise Introduction and Lexicon.” *The Modern Law Review* 76(1). https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2230.12000

- Intellectual Property Office. 2021. “The economic and innovation impacts of trade secrets. UK Government.” https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets
- Kilic, Burcu. 2024. “Into Uncharted Waters: Trade Secrets Law in the AI Era.” CIGI Papers No. 295 (May). https://www.cigionline.org/publications/into-uncharted-waters-trade-secrets-law-in-the-ai-era/
- Matza, Max. 2023. “Google and Canada reach deal to avert news ban over Online News Act.” BBC News. https://www.bbc.com/news/world-us-canada-67571027
- Megwai, Smart. 2024. “Uber Agrees to Share Trip Data with Lagos Government, Addressing Rider Privacy Concerns.” Innovation Village. https://innovation-village.com/uber-agrees-to-share-trip-data-with-lagos-government-addressing-rider-privacy-concerns/
- Moore, Taylor R. 2017. “Trade Secrets & Algorithms as Barriers to Social Justice.” Centre for Democracy and Technology. https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf
- Mylly, Ulla-Maija. 2024. “Trade Secrets and the Data Act.” *International Review of Intellectual Property and Competition Law*, Volume 55 (March). https://link.springer.com/article/10.1007/s40319-024-01432-0
- Ocampo, José Antonio. 2019. “How big tech companies avoid taxes and what can be done about it.” ICRICT. https://www.icrict.com/icrict-in-thenews/2019/1/23/how-big-tech-companies-avoid-taxes-and-what-can-be-done-about-it
- Portuese, Aurelien. 2018. “From Non-Disclosure Agreements to Trade Secrets: Antitrust Implications.” SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188784
- Radauer, Alfred, Nicola Searle, and Martin A. Bader. 2023. “The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors.” World Patent Information no. 73. https://www.sciencedirect.com/science/article/pii/S0172219023000133
- Radauer, Alfred et al. 2022. “Study on the Legal Protection of Trade Secrets in the Context of the Data Economy: Final Report.” European Commission. https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en
- Ruggeroni, Isidora. 2023. “Digital trade agreements cannot prevent AI transparency.” Derechos Digitales. https://www.derechosdigitales.org/22304/digital-trade-agreements-cannot-prevent-ai-transparency/

- Scerri, Simon et al. 2022. “Common European Data Spaces: Challenges and Opportunities.” Data Spaces. https://link.springer.com/chapter/10.1007/978-3-030-98636-0_16
- Segal, Troy. 2024. “What Is Big Data? Definition, How It Works, and Uses.” Investopedia. https://www.investopedia.com/terms/b/big-data.asp
- Stankovich, Miriam. 2024. “Global Toolkit on AI and the Rule of Law for the Judiciary.” UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000387331/PDF/387331eng.pdf.multi
- Thambisetty, Siva et al. 2022. “Addressing vaccine inequity during the covid-19 pandemic: the trips intellectual property waiver proposal and beyond.” *Camb Law J* 16:1-33. doi: 10.1017/S0008197322000241.
- U.S. Department of State. 2024. “United Nations General Assembly Adopts by Consensus U.S.-Led Resolution on Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development.” https://www.state.gov/united-nations-general-assembly-adopts-by-consensus-u-s-led-resolution-on-seizing-the-opportunities-of-safe-secure-and-trustworthy-artificial-intelligence-systems-for-sustainable-development/