Annotated Bibliography on Brazil's Regulations on Privacy, Data Transfers, Access and Cybersecurity

In the past few years, Brazil has had many legal developments in the areas of data protection, government access and cybersecurity that have grown in relevance internationally. This project, started in 2022, focused on creating an accessible English-language annotated bibliography on key Brazilian laws, regulatory frameworks and cases. The summaries provide brief descriptions of legal instruments in the categories of Commercial Privacy, Data Transfers, Law Enforcement and Civil Litigation Access, Cybersecurity Frameworks and Cross-Border Cooperation.

This bibliography was prepared by Chloé Sandoli under the supervision of Richard Salgado and Peter Swire of the Cross-Border Data Forum. Sandoli is an undergraduate student at the H. Milton School of Industrial and Systems Engineering at the Georgia Institute of Technology, and a native speaker of Portuguese. She thanks Fernanda Teixeira Souza Domingos, Federal Prosecutor in Brazil and Member of the ANPR, for assistance in the research phase of this project.

This annotated bibliography documents the following topics:

It is important to preface this bibliography with the judicial context of the Fifth Amendment to the Brazilian Constitution. This amendment sets out individual rights and liberties, including those of "privacy, private life, honor and image of persons." All legislation must work within the confines of this constitutional grant.

I – Commercial Privacy

This section concerns regulations aimed at establishing rules for the collection, use, retention and disclosure of personal data and information about online activity mediated by commercial or third-party players. This includes in some instances how those commercial entities and third parties interact with Brazilian authorities.

1. Brazilian Civil Code (Law 10.460/02)

Documents: official version

The Brazilian Civil Code lays out the rules that address the privacy rights of people, based on the Constitution. Specifically, Civil Code Article 21 sets out the right to privacy and the right to a remedy for its breach:

> Art. 21. The private life of the natural person is inviolable, and the judge, at the request of the interested party, will adopt the necessary measures to prevent or stop an act contrary to this rule.

2. Brazilian Consumer Protection Code (CDC) (Law 8,078/90)

Documents: official version, English version

The CDC has been in effect in Brazil since 1990 and regulates personal information of consumers in databases. Important articles that protect citizens' privacy include:

> Art. 43: Provides that people have the right to access information that exists in registries, forms, and personal consumption data that has been reported about them, as well as their respective sources.
>
> Art. 72: Establishes the sentencing for preventing or hindering consumer access to information about them in registries, databases, files and records.

3. Internet Civil Framework (Marco Civil da Internet) (Law 12.965/14)

a) Overview:

Documents: official version, summarized version (nota da PGR), English version (unofficial - CDD)

The Internet Civil Framework (Law 12.965/14), typically referred to as Marco Civil, is the main legal framework establishing principles and rules governing activities on the internet in Brazil. Enacted in 2014, it regulates many aspects of the use of the internet. These include commercial privacy, net neutrality, intermediary liability, and freedom of expression. Significantly, for purposes here, it also addresses data retention, and compelled production of user data by providers.

With regard to lawful access to user data by the government from service providers, the Internet Civil Framework is analogous to Europe's e-Evidence regulations and the Budapest Convention in that it establishes principles of disclosure and powers held by the government, though it differs in significant ways substantively.

Article 18 of the **Budapest Convention** establishes that a national law has the power to:

> a) demand that an entity in its territory disclose specified computer data to the requesting authority, and
> b) demand that an entity not physically based in its territory but offering its services in the territory disclose subscriber-identifying information.

In the Internet Civil Framework, however, there is no distinction in terms of the types of data that can be demanded depending on whether the entity is within the jurisdiction or not. In particular, Article 11 sets out that, regardless of whether the service provider is physically based in Brazil or is only offering its services in the territory, Brazilian authorities have the power to demand any user data collected, rather than being limited solely to subscriber-identifying information.
Additional differences are described in the "Law Enforcement and Civil Litigation Access" section below.

4. General Data Protection Law (LGPD):

Documents: official version, English translation (IAPP)

The LGPD, Federal Law No. 13,709/2018, is Brazil's first comprehensive data protection law aimed at regulating the treatment of personal, day-to-day data, be that data in physical or digital form. This law is largely based on the GDPR and elaborates on rights provided by previous legislation such as the Consumer Protection Code addressed above.

For example, like in the GDPR, the LGPD in Article 18 provides data subjects certain rights over their data held by a controller. Specifically, the Article grants data subjects the rights to:

"have access to their data; make corrections to incomplete, inaccurate or outdated data and the deletion of personal data processed; portability of the data to another service or product provider; informing about with whom the data has been shared; revoke consent; obtain information about the possibility of not providing consent and the consequences of refusing."

Data Protection Laws of the World – Brazil's LGPD
DLA Piper, January 2023, link

This article summarizes the main context of the law, the scattered preceding legislation, the entities the law applies to and the controversial exceptions of the applicability of the law under Article 4, most notably in the area of national security.

a) LGPD Jurisprudence Report:

PGPD Panel – Jurisprudence Report of the 2nd Year of Effectiveness of the General Data Protection Law
Jusbrasil, April 2023, link (article in Portuguese)

An analysis of 1,789 documents from the 2nd year of the General Data Protection Law shows that judicial decisions involving the law nearly tripled from the first to the second year of the law being in effect. The main issues addressed by the LGPD in courts were in the areas of consumer law, civil responsibilities and security. The report asserts that, in its second year of existence, "the LGPD has taken shape in the courts not only in numbers, but also in the quality of the reasoning … the discussion for general issues of the law has shifted to more specific and practical topics, such as the requirements for treatment of information and accountability."

b) On the limited applicability of the LGPD in courts:

The Limited Effectiveness of the General Law on Personal Data Protection and the Typical Functions of Audit Courts
Instituto Ruy Barbosa, link (paper in Portuguese)

The author argues that the LGPD "is very effective when it comes to the regulation of data processing activities with private companies and public bodies that do not work with the investigation and prosecution of offenses of national interest and protection." Art. 4 limits the reach of the legislation, explicitly stating it does not apply to public security, national defense, or national security, among other areas. The use of personal data for the purpose of investigative activities will require specific legislation.

II – Data Transfers

This section concerns documentation on the proposed bill regarding international data transfers.

1. Proposed International Data Transfer Regulation:

Document: Resolution for International Data Transfer Regulation CD/ANPD (original version in Portuguese)

Brazil's Data Protection Agency (ANPD) published for public consultation its proposed International Transfer of Personal Data Regulation on August 15, 2023. Much like provisions in the GDPR, this proposal aims to regulate international transfers of personal data and the presentation of standard contractual clauses (SCCs). The draft provides that the ANPD will determine which jurisdictions have an adequate level of data protection that will allow the free flow of personal data between Brazil and such countries. The agency will prioritize the review of jurisdictions that provide reciprocal protections. The text does not include provisions relating to limitations of data subject rights such as those under the EU SCCs, which can impose fees for excessive requests or the refusal to comply with a request. Interested parties had until October 14, 2023 to submit contributions to the draft bill.

III – Law Enforcement & Civil Litigation Access

This section concerns documentation and case examples that illustrate how Brazil has been faced with matters involving access to user data from domestic and foreign entities in the context of law enforcement and civil litigation.

1. Interception of Telephone Communication Law (Law 9.296/96)

Document: official text

Law 9.296/96 regulates Item XII, Final Part, of Art. 5 of the Federal Constitution, guaranteeing the secrecy of correspondence and telecommunications.[1] The constitutional clause allows for the breach of secrecy, provided that: 1) the substantive and procedural requirements provided for by law are met; and 2) that the purpose is criminal investigation or the introduction of evidence in criminal proceedings.

This law regulates the interception on both telephone and information technology systems for the purpose of instructing criminal procedures or investigations.[2] Art. 5 notes that the period for surveillance may not exceed 15 days, but it can be renewed upon showing that the evidence is indispensable.

Brazilian Justice has blocked entities from providing internet communication services due to the entities not providing access to data in criminal investigations. The organization *InternetLab* has helpfully classified these cases within two categories, which classification is used in the analysis of two cases in this section.

InternetLab participates in public hearing on cryptography
InternetLab, February 2017, link

“

b) Conflicts of **technical nature**: that it would be impossible to gain access to the content of messages exchanged on apps due to the **obstacles imposed by end-to-end encryption**

b) Conflicts of **judicial nature**: companies indicate that there are limits to the Brazilian jurisdiction over a company headquartered abroad **”**

[1] *Interceptação Telefônica — TJDFT*. Tribunal de Justiça do Distrito Federal e dos Territórios. (2019) https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/interceptacao-telefonica.
[2] *State of Privacy Brazil*. Privacy International. (26 January 2019) https://privacyinternational.org/state-privacy/42/state-privacy-brazil.

Bloqueios.info
2017, link (page in Portuguese)

InternetLab has created a timeline of judicial proceedings that have led, could have led, or can lead to the suspension of internet applications in Brazil, some of which will be used in this bibliography to illustrate the ways in which the Judiciary system has dealt with non-compliance. It is important to note that this resource has only been updated up to 2016.

2. Conflict of Technical Nature - WhatsApp Suspensions, *ADPF 403 and ADI 5527*: a challenge of constitutionality and enforcement

Marco Civil da Internet: Perspectivas de Aplicação e seus Desafios
Escola da Magistratura do Estado do Rio de Janeiro, 2016, link (paper in Portuguese)

The Internet Civil Framework was the target of controversy when it was used to block the messaging application WhatsApp. Four times[3], between February 2015 and July 2016, courts ordered internet service providers to block the domains of the app, on the grounds that the company refused to provide information necessary for criminal investigations.

The issue began when Facebook (now Meta), owner of WhatsApp, initially didn't respond to a data disclosure request for message content issued by the Public Prosecutor's Office, leading to the first 48-hour app suspension. Facebook then explained that it was unable to provide the requested information because the WhatsApp service used end-to-end encryption. Nonetheless, the Judiciary still ordered ISPs in Brazil to suspend the app based on Article 12 of the Internet Civil Framework, Item III, which states it would be possible for the Judiciary to "suspend the activities of a company that does not make their records available."

At the time, some considered the WhatsApp blocks unlawful on multiple grounds. Some viewed the blocks as unconstitutional given they might violate the fundamental precept of freedom[4]. In addition, the blocking of the app may have been based on an incorrect interpretation of the suspension provision in Art. 11 and 12, which is aimed at the collection, storage and processing of personal data records, not app infrastructure. Others defended the decision, highlighting the importance of law enforcement and the existence of practical challenges of the application of the law[5].

---

[3] "Bloqueios.Info." *InternetLab*, 5 Oct. 2017, https://bloqueios.info/en/timeline/.
[4] BRASIL, Supremo Tribunal Federal (Sergipe) "Arguição de Descumprimento de Preceito Fundamental 403", https://www.conjur.com.br/dl/fa/fachin-suspensao-whatsapp-decisao.pdf.
[5] "Folha de S.Paulo: Sem Rastreio, WhatsApp 'Dá Mais Força Para Quem Descumpre a Lei' Diz Juíza." AMAERJ, July 2016, https://amaerj.org.br/noticias/folha-de-s-paulo-sem-rastreio-whatsapp-da-mais-forca-para-quem-descumpre-a-lei-diz-juiza/.

As previously stated, there were four cases involving WhatsApp blocking orders, the last three of which resulted in the block being implemented. The fourth block was ended by Supreme Court Justice Ricardo Lewandovski on July 19, 2016. He ordered the restoration of WhatsApp[6] messaging services on the grounds that blocking the app was a disproportionate measure and went against the principle of freedom (Art. 5 of the Constitution). This last block followed the filing of two constitutional lawsuits: The Unconstitutionality Direct Action (*Ação Declaratória de Inconstitucionalidade* – ADI) nº 5.527 and the Request for Non-Compliance of Fundamental Principles (*Arguição de Descumprimento de Preceito Fundamental* – ADPF) nº 403.

On May 27, 2020, the lawsuits were heard together at the Supreme Court since they both addressed the possibility of courts ordering the suspension of messaging services from apps such as WhatsApp. Below are the summaries of the votes for each one:

Unconstitutionality Direct Action nº 5.527 (ADI nº 5.527)
STF, 2020, link (vote in Portuguese)

In May 2016, the ADI nº 5.527 was proposed by the Liberal Party to question the constitutionality of provisions of the Internet Civil Framework, specifically paragraph 2 of Article 10, which sets out that the content of private communications "can only be made available by court order," and Article 12, Items III and IV, that sets out to protect users' rights by addressing temporary suspension of services in cases of collection, storage, processing and safekeeping of personal data.[7]

On May 27, 2020, Justice Rosa Weber presented her decision upholding the constitutionality of both Articles 10 and 12. In doing so, however, Justice Weber noted that the Articles must be interpreted in accordance with the Constitution,[8] which would not allow for the full suspension of applications as a sanction to "non-compliance with a court order (that would) weaken the privacy protection mechanisms built into the application's architecture." More specifically to the WhatsApp cases, she argues the blocks came from undue applications of Art. 10 and 12, so that these Articles should be interpreted according to the Constitution to leave out any interpretation that a block, as described in Art. 12, could be ordered for not complying with a judicial order that would hinder users' rights.

Petition for Breach of Fundamental Precept 403 (ADPF 403)
STF, 2020, link (vote in Portuguese)

[6] BRASIL, Supremo Tribunal Federal (Sergipe), "Medida Cautelar na Argüição de Descumprimento de Preceito Fundamental 403" https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf.
[7] Atta, Paulo Henrique, and Thiago Moraes. "Summary Report on the Judgement of ADPF No 403 and Adi No 5.527: The Whatsapp Case." *LAPIN*, 31 Aug. 2020, https://lapin.org.br/en-gb/2020/05/29/summary-report-on-the-judgement-of-adpf-no-403-and-adi-no-5-527-the-whatsapp-case/.
[8] Redação ConJur. "Segundo Rosa, Marco Civil Da Internet Não Permite Que WhatsApp Seja Suspenso." *Consultor Jurídico*, 27 May 2020, https://www.conjur.com.br/2020-mai-27/rosa-marco-civil-internet-nao-permite-whatsapp-seja-suspenso/.

Also in May 2016, the ADPF 403 was filed, which discusses whether or not the fourth WhatsApp blocking order decision violated a fundamental precept,[9] Item IX of Article 5 of the Constitution of the Republic, according to which "the expression of intellectual, artistic, scientific and communication activity is free, regardless of censorship or license."
On May 28, 2020, Supreme Court Justice Edson Fachin presented his vote holding that both Item II of Art. 7 and Item III of Art. 12 of the Internet Civil Framework were partially unconstitutional. His opinion was that total suspensions of services violate the fundamental precept of freedom of communication and that the above Articles could not be used to require a provider to grant the government exceptional access to the content of an encrypted end-to-end message.

The petition involved large public hearings, one of which is documented above in the first *Internet Lab* citation. The debate over the enforcement of the Internet Civil Framework is still active, especially since a large part of the law's provisions have not yet been ruled up.

3. Conflict of Judicial Nature - ADC 51: legal conflicts in requests for data stored overseas

This Declaratory Action of Constitutionality (ADC) was aimed at determining whether Brazilian laws could require a provider outside of Brazil to disclose user information even where doing so was illegal in the country of the provider and in spite of diplomatic government-to-government measures in place (like a Mutual Legal Assistance Treaty) through which Brazilian authorities could obtain the information without requiring the provider to break the law of its host country.

ADC51 sessions timeline
STF, May 2023, link (page in Portuguese)

2020: Facebook *amicus curiae* for ADC51
Ação Declaratória de Constitucionalidade nº 51 - Facebook Brasil, link (statement in Portuguese)

In 2020, representatives from Yahoo, Facebook, and other national business associations attended public hearings and contributed as *amici curiae* to support the approval of MLATs as valid.

September 2022: Supreme Court – Application of MLAT (09/29/2022 session)
Jota, September 2022, link (article in Portuguese)

Some courts of appeal understood that the data could only be obtained by letters rogatory or a cooperation agreement. The Superior Court of Justice (STJ), however, understood that access

[9] Valente, Fernanda. "Bloqueio Judicial Do Whatsapp É Inconstitucional, Diz Fachin." *Consultor Jurídico*, 28 May 2020, https://www.conjur.com.br/2020-mai-28/bloqueio-judicial-whatsapp-inconstitucional-fachin/.

to this data can also be given by a court order directed to the company's branch headquarters or subsidiary in the country, even if they do not have custody or control of the data (through the Internet Civil Framework). Facebook, Yahoo, the Institute for Reference on Internet and Society (IRIS), and the Society of Technology Users (Sucesu Nacional) were admitted as interested parties in the case.

2023: ADC51 Supreme Court Justice Gilmar Mendes's Vote
Ação Declaratória de Constitucionalidade nº 51 - Gilmar Mendes, link (vote in Portuguese)

The ADC51 trial was finalized, declaring, by unanimous vote, that both Art. 11 of the Internet Civil Framework and MLAT regulations are constitutional. It was decided that the fact that information may be available through an MLAT request or letters rogatory doesn't mean that those mechanisms must be used. The law may properly require that technology companies maintain representation in Brazil and answer directly to the Brazilian Judiciary, at least with regard to data collected in Brazil.

It was also decided that "in the cases of data collection and processing activities in the country, given possession or control of the data by a company with representation in Brazil and of crimes committed by individuals located in national territory, with communication of this decision to the Legislative and Executive branches, so that they may adopt the necessary measures to improve the legislative framework, with the discussion and approval of the General Law of Data Protection for Criminal Purposes (LGPD Criminal) project and of new bilateral or multilateral agreements for obtaining data and electronic communications, such as, for example, the execution of the Executive Agreement defined from the Cloud Act, all in the terms of the Rapporteur's vote."

4. Resolutions on Administrative Sanctioning and Imposition of Penalty Guidelines for ANPD

Regulation of the Inspection and Sanctioning Administrative Proceedings (CD/ANPD Nº 1):
Documents: official text

In 2021, the ANPD approved the Regulation of the Inspection Process and the Administrative Sanctioning Process, which establishes the inspection activities carried out by the authority. These include monitoring, guidance and audits to bring processing agents back into compliance with the LGPD. It also includes investigating infractions and punishing those responsible through the application of the administrative sanctions provided for in the LGPD.

Regulation on the Measurement and Imposition of Penalties (CD/ANPD Nº 4):
Documents: official text

In 2023, the Regulation on the Measurement and Application of Administrative Sanctions, as provided for in Article 53 of the General Data Protection Law, was approved. This new regulation strengthens the ANPD's enforcement activities by determining the factors for assessing fines in the event of infringements, as well as establishing more objective criteria for assessing violations.[10] One of the guideline's highlighted features is the transparent methodology to calculate fines depending on the level of infractions.

5. Documentation on Data Protection and AI Regulation

Insights into Brazil's AI bill and its Interaction with Data Protection Law: key takeaways from the ANPD's webinar
Future of Privacy Forum, July 2023, link

Brazil's bill nº2338, currently under consideration by a Senate Commission, aims to regulate artificial intelligence (AI) systems in Brazil. This bill originated from efforts by the Senate, ANPD, and previously proposed bills such as the Regulatory Framework for Artificial Intelligence (Bill No. 21/2020), and bills No. 5.051/2019 and 872/2021.

The bill touches on the importance of centering technology on the human person, respect for human rights and democratic values, privacy, justice, equity and inclusion, transparency, explainability, intelligibility and auditability. The article provides additional insights into the ANPD and further AI agenda in Brazil.

More recently, Senate President Rodrigo Pacheco reported that Bill 2338/2023 should be voted on by the end of April 2024[11].

Personal Data Protection and Criminal Investigations
Associação Nacional dos Procuradores da República, 2020, link (papers in Portuguese)

The collection of articles above by the National Association of Prosecutors of the Republic further elaborates on issues of data protection in criminal investigations.

[10] Kujawski, F. F., Sessa, L. F., & Santos, L. M. (2023, March 15). *Desafios relacionados ao Regulamento de Dosimetria da ANPD*. JOTA Info. https://www.jota.info/opiniao-e-analise/artigos/desafios-relacionados-ao-regulamento-de-dosimetria-da-anpd-15032023.

[11] DataCenterDynamics, "Projeto de lei para regular IA no brasil Deve Ser votado Até Abril", *DCD*, 6 February 2024, https://www.datacenterdynamics.com/br/not%C3%ADcias/presidente-do-senado-diz-que-projeto-de-lei-para-regular-ia-deve-ser-votado-ate-abril/.

IV – Cybersecurity Frameworks

This section is concerned with the current cybersecurity frameworks and strategies present in Brazil.

a) Overview:

Cybersecurity Strategy in Brazil: past, present and future
Barbara Marchiori de Assis, March 2020, link (article in Portuguese)

Before the official strategies and policies above were instituted, the Institutional Security Cabinet (GSI) of the Presidency published various documents from 2010 to 2015 on cybersecurity measures such as the *Reference Guide for the Security of Critical Information Infrastructures.* Brazil was also very active in the UN-GGE (Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security), having participated in five of the six meetings since 2004. In 2018, the first National Cybersecurity Strategy was enacted, defining the guidelines for cybersecurity within the Federal Public Administration, subsequently being replaced by the broader current PNSI. The relevance of such documents only grows as "recent cybersecurity reports show that Brazil is one of the countries with the highest number of cybercrimes, affecting more than 60 million people and causing losses estimated at more than 20 billion dollars."

1. National Information Security Policy (PNSI)

Documents: official text

Evaluation of the national information security policy by analytic hierarchy process
School of Information Science of UFMG, December 2022, link (paper in Portuguese)

The decree Nº 9.637 was published in December 2018 as the Política Nacional de Segurança da Informação / National Information Security Policy (PNSI). It intends to guide the governance of information security, covering I - cyber security; II - cyber defense; III - physical security and protection of organizational data; and IV - actions to ensure the availability, integrity, confidentiality and authenticity of information. This decree also notably includes the incentive to academic research related to information security.

2. National Cybersecurity Strategy (E-Ciber)

Documents: official text

The Estratégia Nacional de Seguraça Cibernética / National Cybersecurity Strategy, mostly known as E-Ciber, is the first document of the National Security Strategy, consisting of instruments for the implementation of the PNSI pertaining to cybersecurity. It is understood that other modules pertaining to cyber defense, critical infrastructure security, sensitive information security, and data leakage protection will be released in the future.

E-Ciber brings a governance model through a national cybersecurity system and preparation of a draft bill on cyber security, under the coordination of the Institutional Security Cabinet. Additionally, the plan takes into consideration the protection of states and small companies that drive a significant portion of the Brazilian economy, even though some objectives still lack clearer plans for applicability.

3. Brazilian Criminal Code - electronic fraud and hacking

Document: official text

Art. 171 of the Brazilian Criminal Code establishes rules against fraud, including electronic fraud. It establishes penalties for "obtaining, for oneself or for others, an illicit advantage, to the detriment of others, by inducing or maintaining someone in error, through artifice, ruse, or any other fraudulent means."

Art. 154-A regulates hacking. It establishes that "hacking into someone else's computer device, whether or not connected to a computer network, in order to obtain, tamper with or destroy data or information without the express or tacit authorization of the user of the device, or to install vulnerabilities in order to obtain an illicit advantage." [12]

Articles 305 and 307 can also be applied in cases of hacking and cyber threats.

4. Additional Supporting Legislation / Documentation:

Department of Information Security and Cybernetics: English versions of relevant legislation:
Presidency of the Republic Office of Institutional Security, link (page in Portuguese)

Information Security Glossary
Presidency of the Republic Office of Institutional Security, link (page in Portuguese)

[12] "Invasão de Computador." *Tribunal de Justiça Do Distrito Federal E Dos Territórios*, https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/invasao-de-computador#:~:text=O%20C%C3%B3digo%20Penal%2C%20em%20seu.

This website of the Department of Information Security and Cybernetics (Departamento de Segurança da Informação e Cibernética) features additional laws and decrees from 2014 to 2021 related to cyber incident management, cloud regulation, etc., and a comprehensive Information Security Glossary.

V – Cross-Border Cooperation

This section is concerned with recent international cooperation between Brazil and other nations on matters of digital transformation and cross-border policy.

1. Brazil's G20 Presidency and Digital Governance

Brazil's Role in Shaping the Digital Transformation
Wilson Center, link, February 29, 2024

Brazil's priority issues for the G20 presidency are poverty, sustainable development and global governance. Focusing on the last, in an interview for the Wilson Center, Luanna Roncaratti, Brazil's Deputy Secretary of Digital Government at the Management and Innovation Ministry, discussed some of the government's main priorities. Improving digital public infrastructure is a focus, and Roncaratti also highlighted interoperability by noting that Brazil is "committed to advancing our data governance and data sharing initiatives." On data governance specifically, when asked about global safeguards around data, Roncaratti highlighted the need for a "regulatory environment that ensures the ethical use of data, preserves citizens' right to privacy and avoids predatory use of data." Collaborations with Denmark, Germany and other nations were cited in the article as fruitful partnerships around digital transformation.

2. EU – Brazil

The EU and Brazil strengthen their digital cooperation
European Commission press release, link, March 21, 2024

On March 20, 2024, the European Union (EU) and the Government of Brazil held their 12th Digital Dialogue in Brazil and agreed to cooperate on a variety of projects such as data protection and international data flows. See the full communiqué of the EU and Brazil.