

ARTICLE

INTERNATIONAL TRANSFERS OF PERSONAL DATA IN LATIN AMERICA: FROM THE BRUSSELS EFFECT TO THE WASHINGTON EFFECT

Pablo A. Palazzi*

ABSTRACT

This Article examines international data transfer regimes in Latin America through the competing influences of the Brussels Effect and what it conceptualizes as the Washington Effect. First, it shows how EU data protection law has shaped not only primary legislation in the region, but also technical rules governing cross-border data flows. Second, it analyzes how the United States has sought to project its long-standing commitment to free data flows through trade agreements and soft-law mechanisms such as the CBPR system, rather than through comprehensive privacy legislation. This Article is the first to conceptualize the US strategy of embedding de facto adequacy determinations within trade agreements under the label of the Washington Effect, and to assess its projected impact on the global data protection ecosystem and the traditional dominance of the Brussels Effect. Finally, this Article situates these developments within broader geopolitical tensions between trade liberalization and privacy-based data transfer restrictions, and the effect on current transfer methods, with significant implications for the future of cross-border data governance in Latin America and beyond.

* LL.M. Fordham Law School (2000). Professor of Law and Director of the Center for Technology and Society (CETyS) at Universidad de San Andrés (Buenos Aires, Argentina). The author is a partner at Allende & Brea in Buenos Aires, Argentina, where he heads the TMT Law practice. His practice and academic work focus on TMT law, data protection, AI law, and dispute resolution matters. I thank the staff of the Fordham International Law Journal for their excellent editorial assistance. All errors remain my own. The author can be reached at ppalazzi@udesar.edu.ar.

I.INTRODUCTION.....	1155
II.THE BRUSSELS EFFECT IN LATIN AMERICA.....	1155
A. The Brussels Effect	1155
B. The Adoption of the EU Model in Latin America (1999–2026)	1158
1. Evolution of Data Protection Laws in the Region 1159	
2. Data Protection Authorities	1163
3. Secondary Regulations of Privacy	1172
4. International Transfers of Personal Data in Latin America	1174
5. Adequacy Determinations of Latin American Countries	1179
III.THE “WASHINGTON EFFECT”: THE REGULATORY ALIGNMENT THROUGH TRADE AGREEMENTS.....	1181
A. The United States’ Position on International Data Flows.....	1181
B. Unilateral Recognition of Adequacy of the United States in Trade Agreements.....	1184
C. The Alternative of Piggybacking on the Existing EU– US Adequacy Agreements or EU Adequacy Determinations	1190
D. The Promotion of the Cross-Border Privacy Rules System	1195
IV.THE TRADE AND/OR PRIVACY DEBATE: GEOPOLITICAL TENSIONS AND THE FUTURE OF CROSS-BORDER DATA RULES IN LATIN AMERICA.....	1198
A. The “Washington Effect” as a Counter-Narrative to the Brussels Effect.....	1198
B. The Dilution of “Adequacy” as a Normative Concept 1201	
C. The Internal Implementation of Unilateral Recognition in Trade Agreements: Future Challenges Ahead?	1206
D. A Proposal: The Need to Regulate the Collection of Personal Data Online	1210
V.CONCLUSION	1211

I. INTRODUCTION

The rapid proliferation of data protection frameworks across Latin America has generated underexplored tensions—between domestic regulatory ambitions and transnational data flows, between convergence and fragmentation, and between competing geopolitical interests.

Part II analyzes the Brussels Effect as a driver for data protection legislation in the region, examining both the general adoption of European regulatory models and the specific mechanisms through which General Data Protection Regulation (“GDPR”)-inspired standards have been absorbed and adapted.

Part III turns to the United States and examines efforts to align US legal frameworks with Latin American data protection requirements, with particular attention to the role of trade agreements and the Cross-Border Privacy Rules (“CBPR”) system—an indirect form of regulatory influence that this Article conceptualizes as the Washington Effect. This Article is the first to examine the US strategy of embedding adequacy determinations into trade agreements—conceptualized here as the Washington Effect—and to project its implications for Latin America and the global data protection ecosystem and for the regulatory influence traditionally associated with the Brussels Effect.

Part IV situates these developments within a broader geopolitical frame, exploring tensions between the free flow of information and the growing emphasis on privacy regulation and data localization.

II. THE BRUSSELS EFFECT IN LATIN AMERICA

A. The Brussels Effect

Long before “the Brussels Effect” became a term of art, scholars were already tracing how the Internet and the EU’s 1995 Data Protection Directive were reshaping global privacy governance.

Joel Reidenberg mapped early on how many national systems converged around fair information practice principles while simultaneously restricting transfers to destinations lacking sufficient protection—an architecture the Directive turned into an

operational, market-access constraint.¹ In his account, “adequacy” transformed cross-border transfers from a policy aspiration into a practical compliance fork in the road: States and firms seeking stable data relations with Europe would either elevate domestic safeguards or devise negotiated, bespoke mechanisms to keep data moving.²

At the same time, other early commentators highlighted both the disruptive reach and the institutional adaptations the Directive was already catalyzing, as reflected in the views discussed below. Gregory Shaffer argued that European Union and international rules were pushing an “upward ratchet” in US practice even before comprehensive federal legislation emerged, while Fred Cate framed the Directive as a sweeping, rights-based regime that projected European preferences outward and sharpened conflict with the US sectoral, speech-protective model.³ Peter Swire and Robert Litan, writing as the Directive took effect, treated the adequacy restriction as a potential obstacle to transatlantic commerce and a driver of policy workarounds—precisely the kind of pressure that later materialized in negotiated transfer mechanisms.⁴ Paul Schwartz likewise emphasized that the Directive’s “adequacy” lever institutionalized a transatlantic collision, making international data flows a site of sustained legal and political negotiation rather than mere private ordering.⁵

Two decades later, Bradford’s “Brussels Effect” supplied the unifying theory: The European Union can export regulatory standards globally through unilateral market regulation and the

1. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); see also Joel R. Reidenberg, *The Globalization of Privacy Solutions: The Movement Towards Obligatory Standards for Fair Information Practices*, in VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 217 (Colin J. Bennett & Rebecca Grant eds., 1999).

2. Reidenberg, *Lex Informatica*, *supra* note 1.

3. See Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT’L L. 1 (2000); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 176–86 (1999); see also FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 65–89 (2000).

4. See PETER P. SWIRE & ROBERT E. LITAN, *NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE* 7–15 (1998).

5. See Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995).

incentives of access to EU consumers and firms, without formal treaty harmonization.⁶

Yet Latin America's GDPR-adjacent trajectory is not explained by market leverage alone. As Bennett's comparative work underscores, there are broader structural pressures toward policy convergence around baseline data-protection principles; and in Latin America, those pressures have been reinforced by adequacy-style transfer conditionality, commercial interoperability goals,⁷ and the region's civil-law receptivity to European regulatory templates.⁸

To explain the Brussels Effect in Latin America and its impact on data protection, it is useful to distinguish several layers of analysis.

At the first and most visible level, it manifests in the adoption of comprehensive data protection statutes modeled on the European framework—drawing both from the foundational 1995 Data Protection Directive and, more recently, from the GDPR as the contemporary benchmark.

At a second level, the Brussels Effect can be observed in the establishment of independent data protection authorities (“DPAs”) tasked with enforcement and oversight. The creation of such agencies represents a significant institutional dimension of the Brussels Effect: It is not merely a matter of transplanting legal norms, but of building the institutional infrastructure— independent, specialized, and empowered—that the European model presupposes and that gives those norms practical effect. In turn, these agencies often work closely with European regulators, particularly with the Spanish Data Protection Authority.

At a third, more granular level, the Brussels Effect extends beyond the transplantation of legislative architecture and institutional design to encompass the absorption of secondary

6. See ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* (2020).

7. See COLIN J. BENNETT, *REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES* (1992).

8. See Joel Reidenberg, Prologue to PABLO A. PALAZZI, *LA TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES Y LA PROTECCIÓN DE LA PRIVACIDAD*, at 43 (2001). In the prologue to this book, Professor Joel Reidenberg once again demonstrated the prescience of his work, observing that the newly enacted data protection statutes in Argentina and Chile provide concrete validation of his thesis on the worldwide diffusion of European data protection norms. *See id.*

regulatory elements: Specific GDPR concepts, definitional structures, and enforcement mechanisms find their way into national law, while guidelines, opinions, and recommendations issued by the European Data Protection Board (“EDPB”) increasingly serve as interpretive references for regulators and courts in jurisdictions far beyond the EU’s territorial reach.

The adequacy decision has functioned as a powerful regulatory magnet, drawing third countries into the data protection orbit of the European Union.

European influence on Latin American data protection has proven deeper than the proliferation of GDPR-inspired statutes might suggest. The transplant has carried not just legal form but legal meaning—shaping the interpretive frameworks that regulators bring to enforcement, the doctrinal tools that courts deploy, and the normative assumptions that underpin policy choices. It is this substantive dimension of convergence, more than any formal alignment of legislative text, that defines the true reach of the Brussels Effect.

B. The Adoption of the EU Model in Latin America (1999–2026)

The adoption of EU-inspired data protection standards across Latin America should not be understood as an automatic or uniform process. Important structural differences exist between the legal architecture of many Latin American jurisdictions and that of the European Union, and not all institutional features of the European system can be directly transplanted or made to function in the same manner. Nonetheless, at a general level, the regulatory frameworks that have emerged in the region tend to converge toward a predominantly European model of personal data protection.

The adoption of the European data protection model in Latin America can be broadly categorized into two phases: First-generation laws and second-generation laws. The former laws were largely inspired by the 1995 EU Data Protection Directive and the Spanish data protection legislation,⁹ while the latter laws are primarily based on the GDPR.

9. See Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (B.O.E. 1992, 262) (Spain); see also Ley

1. Evolution of Data Protection Laws in the Region

One way to assess the magnitude of the Brussels Effect in Latin America is by examining the number and content of personal data protection laws adopted throughout the region.

The region entered the era of first-generation laws with a pre-existing normative landscape: Chile enacted its data protection law in 1999.¹⁰ One year later, Argentina enacted its Personal Data Protection Law,¹¹ modeled largely on the European Data Protection Directive of 1995,¹² and subsequently obtained adequacy recognition from the European Commission in 2003.¹³

In the following decade, Uruguay,¹⁴ Mexico,¹⁵ Costa Rica, and Peru¹⁶ joined the data protection club with first-generation laws based on the old model of the EU directive of 1995.

The period of second-generation data protection laws in Latin America started in 2020, when Brazil's Lei Geral de Proteção de Dados ("LGPD"), enacted in 2018, entered into force; it was followed by Ecuador, Panama, Chile, and Paraguay¹⁷ enacting regulations closely based on the GDPR.

Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. 1999, 298) (Spain).

10. See Law No. 19628 art. 4, Agosto 28, 1999, Diario Oficial [D.O.] (Chile).

11. See Law No. 25326, Protección de los Datos Personales, Oct. 4, 2000, B.O. (Arg.).

12. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. [L 119] 1 [hereinafter GDPR].

13. See Commission Decision 2003/490/EC of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, 2003 O.J. (L 168) 19. On January 15, 2024, the European Commission confirmed that Argentina continues to provide an adequate level of data protection for personal data transferred from the EU. See Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC, at 4, COM (2024) 7 final (Jan. 15, 2024).

14. See Law No. 18331, Protección de Datos Personales y Acción de Habeas Data, Agosto 11, 2008, Diario Oficial [D.O.] (Uru.).

15. See Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP], Diario Oficial de la Federación [DOF] 05-07-2010 (Mex.).

16. See Law No. 29733, Ley de Protección de Datos Personales, Julio 3, 2011, Diario Oficial El Peruano [El Peruano] (Peru).

17. See Law No. 7593/2025, Protección de Datos Personales en la República del Paraguay, Noviembre 27, 2025, Gaceta Oficial (Para.).

In the next decade, some countries, including Uruguay,¹⁸ Peru,¹⁹ and Chile,²⁰ updated their data protection frameworks to align them more closely with the GDPR, resulting in what this Article refers to as second-generation laws.

In some jurisdictions, such as Uruguay, the personal data protection framework was updated through incremental reforms adopted over time, often incorporated into successive annual budget laws.²¹ These updates were also influenced by peer pressure from neighboring countries, as governments seek to keep their regulatory frameworks aligned with regional developments.

Other countries, however, have failed to update their data protection laws, despite several attempts. Argentina, for example, has undertaken efforts to modernize its Personal Data Protection Law No. 25,326 of 2000—a statute that is now nearly a quarter century old—on two occasions without success. The first attempt took place in 2017 through a reform bill drafted after a year-long public consultation process led by then DPA director Eduardo Bertoni.²² A second effort followed in 2022, when a new reform bill was prepared by the current DPA through a participatory drafting process involving academia, the private sector, and civil society

18. Uruguay has progressively amended its data protection law through successive reforms incorporating elements inspired by the GDPR.

19. In Peru, the reform of the first-generation data protection law, aimed at aligning the framework with the European General Data Protection Regulation, was enacted by executive decree, a legislative technique that attracted criticism regarding its procedural legitimacy.

20. Chile enacted Law No. 21,719 on the Protection of Personal Data in 2024, modernizing its data protection framework and aligning it with international standards, particularly the European GDPR. The law will become fully effective and enforceable on December 1, 2026, following a transitional implementation period.

21. Since its enactment in 2008, Uruguay's Personal Data Protection Law (Law No. 18,331) has been amended on three occasions, all through omnibus legislation rather than standalone data protection reform. The first amendment was introduced through the National Budget Law No. 19,355 (2015–2019), which made structural adjustments to the URCDP's institutional framework. The most substantive reform came through the Rendición de Cuentas Law No. 19,670 (2018), which entered into force in January 2019 and introduced four articles updating the original statute, most notably a revised accountability principle under Article 12, now extending liability to both data controllers and processors and incorporating concepts drawn directly from the GDPR such as privacy by design, privacy by default, and data protection impact assessments. A third set of amendments followed through the National Budget Law No. 19,924 (2020–2024), which added a statutory definition of biometric data to Article 4 and introduced provisions on audiovisual content distribution with data protection implications.

22. See Eduardo Bertoni, *El impacto de una ley que nació anticuada*, in 1 PROTECCIÓN DE DATOS: DOCTRINA Y JURISPRUDENCIA 27 (Pablo A. Palazzi ed., 2020).

organizations.²³ This last proposed legislation tracked the GDPR closely, incorporating its core architecture of legal bases for processing, enhanced data subject rights, mandatory data protection officers, and risk-based accountability obligations.²⁴ The bill,²⁵ however, failed to advance in the National Congress, leaving Argentina with an aging regulatory framework that increasingly diverges from contemporary international standards. The DPA is currently working on a third bill to be sent to Congress at the end of the year.

In some jurisdictions, such as Brazil, the process produced a comprehensive legal instrument—the Lei Geral de Proteção de Dados of 2018²⁶—that consciously mirrors the GDPR’s structural architecture,²⁷ adopting even more legal bases for processing,²⁸ parallel data subject rights, and an institutional model centered on a regulatory agency.²⁹

Another notable development in the regional data protection landscape has been the progressive adherence of Latin American

23. See, e.g., Agencia de Acceso a la Información Pública [AAIP], Resolución 119/2022, Sept. 12, 2022, B.O. (Arg.).

24. See BEATRIZ ANCHORENA, AAIP, PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES 8 (2024).

25. See Agencia de Acceso a la Información Pública [AAIP], *Propuesta de Anteproyecto de Ley de Protección de Datos Personales* (Aug. 30, 2022), https://www.argentina.gob.ar/sites/default/files/2022/09/propuesta_de_anteproyecto_de_ley_vf.pdf [<https://perma.cc/C74M-LBLP>] [hereinafter *AAIP Anteproyecto 2022*] (preliminary draft presented following participatory roundtables conducted in July and August 2022; superseded by the bill submitted to Congress as Mensaje No. 87/2023).

26. See Lei Geral de Proteção de Dados Pessoais [LGPD], Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).

27. See Abigayle Erickson, *Comparative Analysis of the EU’s GDPR and Brazil’s LGPD: Enforcement Challenges with the LGPD*, 44 BROOK. J. INT’L L. 859 (2019).

28. See LGPD art. 7 (Braz.). The Brazilian General Data Protection Law establishes a broader set of legal bases for the processing of personal data than those recognized under the GDPR. Article 7 of the LGPD provides ten distinct legal grounds for processing, including: Consent of the data subject; compliance with a legal or regulatory obligation; the execution of public policies by public administration bodies; the performance of studies by research entities; the execution of a contract or preliminary contractual procedures requested by the data subject; the exercise of rights in judicial, administrative, or arbitration proceedings; the protection of life or physical safety; the protection of health by health professionals or entities; the legitimate interests of the controller or a third party; and the protection of credit. *Id.* This broader catalogue reflects the Brazilian legislature’s attempt to adapt the European model of data protection to local legal and economic realities while maintaining overall conceptual alignment with the GDPR.

29. LGPD art. 55-A (Braz.) (creating the Autoridade Nacional de Proteção de Dados (ANPD), Brazil’s national data protection authority).

countries to the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, known as Convention 108.³⁰ Although originally conceived as a European treaty, Convention 108 was opened to accession by non-member states of the Council of Europe, and several Latin American jurisdictions have availed themselves of this mechanism as a means of signaling their commitment to internationally recognized data protection standards.³¹ Uruguay became the first Latin American country to accede to Convention 108 in 2013,³² followed by Argentina, and then Mexico. Brazil, Ecuador, and Chile are also working on the approval of Convention 108. This gradual accession illustrates the growing influence of European data protection standards beyond the European continent and reflects the increasing willingness of Latin American jurisdictions to align their legal frameworks with international privacy instruments developed within the Council of Europe system.

The following chart provides a chronological overview of the adoption of personal data protection laws across Latin America:

Year	Country	Name of the Law
1999	Chile	Law No. 19,628 on the Protection of Private Life
2000	Argentina	Law No. 25,326 on the Protection of Personal Data
2008	Uruguay	Law No. 18,331 on the Protection of Personal Data and Habeas Data Action

30. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention 108].

31. Convention 108, *supra* note 30; Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Oct. 10, 2018, C.E.T.S. No. 223 [hereinafter *Convention 108+*]; see *Chart of Signatures and Ratifications of Treaty 108*, COUNCIL OF EUR., <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108> [https://perma.cc/JL8Z-NDCW].

32. The adhesion of Uruguay was announced when the country was the host to the Global Privacy Assembly in Punta del Este in 2013.

Year	Country	Name of the Law
2010	Mexico	Federal Law on the Protection of Personal Data Held by Private Parties (replaced in 2025)
2012	Colombia	Law No. 1,581 on the Protection of Personal Data
2013	Peru	Law No. 29,733 on the Protection of Personal Data
2016	Costa Rica	Law No. 8,968 on the Protection of Individuals with Regard to the Processing of Personal Data
2020	Brazil	General Data Protection Law (Lei Geral de Proteção de Dados), Law No. 13,709/2018
2021	Ecuador	Organic Law on the Protection of Personal Data
2022	Panama	Law No. 81 on the Protection of Personal Data
2025	Paraguay	Law No. 7,593/2025 on the Protection of Personal Data

2. Data Protection Authorities

The reach of the Brussels Effect in Latin America can also be assessed through the growing number of data protection authorities actively operating across the region, as well as through the specific institutional influence of regional coordination mechanisms.

This institutional dimension has progressively taken shape across Latin America, where countries such as Argentina, Uruguay, Peru, Mexico, Brazil, Colombia, Ecuador, Costa Rica, Panama, and Chile have established regulatory frameworks that include

independent supervisory authorities entrusted with enforcing data protection rules.

In this respect, the Ibero-American Data Protection Network (Red Iberoamericana de Protección de Datos, “RIPD”) plays a central role.³³ The RIPD—which brings together supervisory authorities from Spain, Portugal, and the Spanish- and Portuguese-speaking countries of Latin America—has served as a vehicle for the transmission of European regulatory concepts and enforcement approaches into the regional administrative culture. It provides a forum for coordination, exchange of best practices, and joint enforcement initiatives across the region.

While the Ibero-American Data Protection Network is not an autonomous supranational body comparable to the European Data Protection Board, and cannot issue mandatory regulations, its role in the region has become increasingly significant.

Through cooperation among national data protection authorities—and with the support and technical assistance of institutions such as the Spanish Data Protection Agency and other European authorities—the Network has progressively strengthened regulatory dialogue and policy coordination across Latin America by creating working groups on certain matters, coordinating enforcement action across the region, drafting policy documents on current issues such as COVID-19 and personal data,³⁴ cloud computing,³⁵ artificial intelligence,³⁶ and a model

33. The Network has functioned as a key vector for the diffusion of European data protection principles, a role further reinforced by the fact that its permanent secretariat is held by Spain’s Data Protection Authority (Agencia Española de Protección de Datos, AEPD). This institutional configuration has contributed to the consolidation and alignment of regulatory practices in the region with European data protection standards.

34. Red Iberoamericana de Protección de Datos (RIPD), *RIPD Recommendations for the Processing of Personal Health Data During the Pandemic* [*Recomendaciones de la RIPD para el tratamiento de datos personales sobre la salud en tiempos de pandemia*] (Apr. 2021), <https://www.redipd.org/documento/recomendaciones-ripd-tratamiento-datos-personales-salud-en-pandemia.pdf> [<https://perma.cc/HX6Q-U6Z7>].

35. Red Iberoamericana de Protección de Datos (RIPD), *Recommendations for the Processing of Personal Data Through Cloud Computing Services* [*Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube*] (Apr. 2021), <https://www.redipd.org/documento/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf> [<https://perma.cc/PWW7-UMX2>].

36. Red Iberoamericana de Protección de Datos (RIPD), *General Recommendations for the Processing of Personal Data in Artificial Intelligence* (June 21, 2019), <https://www.redipd.org/en/document/guide-general-recommendations-processing-personal-data-ai-en.pdf> [<https://perma.cc/XY58-6DQG>].

agreement for international data transfers with an explanatory guide for using and implementing the models.³⁷

In this context, the influence of European data protection standards continues to expand at multiple levels, illustrating how the Brussels Effect extends beyond formal legal harmonization into institutional cooperation and regulatory practice.³⁸

In addition, all the Latin American authorities actively participate in the Global Privacy Assembly as accredited members,³⁹ which integrates them into the global network of data protection regulators, and facilitates cooperation on enforcement as well as awareness of the constant regulatory and policy developments occurring in the field of personal data protection.

The establishment of independent data protection authorities in Latin America has not been a straightforward process. In several Latin American countries, constitutional and institutional constraints initially limited the creation of autonomous supervisory bodies. In Mexico, for example, the establishment of an independent data protection authority ultimately required constitutional reform,⁴⁰ while in Chile, attempts to introduce

37. Red Iberoamericana de Protección de Datos (RIPD), *Implementation Guide on Model Contract Clauses for International Personal Data Transfers (IPDT)* (Sept. 27, 2022), <https://www.redipd.org/en/document/implementation-guide-on-model-contract-clauses-ipdt-en.pdf> [<https://perma.cc/GDU6-Y6PH>].

38. See *List of Accredited Members*, GLOB. PRIV. ASSEMBLY, <https://globalprivacyassembly.com/participation-in-the-assembly/list-of-accredited-members/> [<https://perma.cc/T9MQ-N5X3>] (listing membership of the following Latin American countries: Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, and Uruguay). In addition, Mexico was historically a member through its autonomous guarantor body, the INAI, but following structural reforms and the abolition of the institute's board, its membership and international representation status remain under accredited status review.

39. See *id.*

40. Mexico granted constitutional autonomy to its federal transparency and data protection authority through a constitutional reform adopted in 2014, which transformed the Federal Institute for Access to Information (IFAI) into the National Institute for Transparency, Access to Information and Personal Data Protection (INAI). See Constitución Política de los Estados Unidos Mexicanos, CPEUM, art. 6, Diario Oficial de la Federación [DOF] 05-02-1917, últimas reformas DOF 07-02-2014 (Mex.); see also LUIS GUSTAVO PARRA NORIEGA, *HACIA UNA NUEVA AUTORIDAD ESPECIALIZADA EN PROTECCIÓN DE DATOS PERSONALES EN MÉXICO* (2022).

similar institutional reforms⁴¹ have encountered political resistance and were at one stage rejected by popular vote.⁴²

In the case of Mexico, the data protection authority was an autonomous agency enshrined in the Federal Constitution. It held broad competence in data privacy, transparency, and access to information.⁴³ Furthermore, the agency held key leadership positions within both the Ibero-American Data Protection Network and the Global Privacy Assembly (“GPA”) for many years.⁴⁴ But in late 2024, the Mexican government proceeded to eliminate the data protection agency, as part of a constitutional reform to reduce costs and centralize power.⁴⁵ Responsibilities for data protection and public information requests were moved to the executive branch’s Secretariat of Anti-Corruption and Good Governance.

In other jurisdictions, the challenge took a different form. Both Argentina and Brazil enacted comprehensive data protection statutes that contemplated the creation of supervisory authorities; however, in each case, the respective presidents vetoed the provisions granting institutional autonomy to those authorities, thereby allowing the executive branch to establish them within its own administrative structure. As a result, the supervisory bodies initially lacked the degree of independence required by the European model of data protection governance. Over time,

41. The 2022 draft Chilean Constitution, ultimately rejected in a national referendum, included a provision establishing a data protection authority and granting it constitutional status.

42. See Patricia Mazzei, *Chileans Reject New Constitution, Dealing Blow to Left*, N.Y. TIMES (Sept. 4, 2022), <https://www.nytimes.com/2022/09/04/world/americas/chile-constitution-no.html> [<https://perma.cc/2XTB-BULC>].

43. Gregory Michener et al., *Lessons from the Dissolution of Mexico’s Information Commission*, 38 GOVERNANCE e70031 (2025); see also Fernando Nieto Morales, *The Elimination of INAI: A Blow to Transparency and Accountability in Mexico*, WILSON CTR. (Nov. 21, 2024), <https://www.wilsoncenter.org/article/elimination-inai-blow-transparency-and-accountability-mexico> [<https://perma.cc/4V94-DZKM>].

44. The Mexican DPA hosted the forty-third edition of the Global Privacy Assembly in Mexico City. This hybrid event focused on the intersection of new technologies and human rights. Following the 2021 conference, INAI’s Commissioner Blanca Lilia Ibarra Cadena was elected as Chair of the Global Privacy Assembly. Under Mexico’s involvement, the GPA adopted resolutions focused on children’s digital rights, government access to data, and data sharing for the public good.

45. See James Wagner & Emiliano Rodríguez Mega, *Why Mexico Is Eliminating Independent Watchdog Agencies*, N.Y. TIMES (Nov. 28, 2024), <https://www.nytimes.com/2024/11/28/world/americas/mexico-senate-watchdog-agencies.html> [<https://perma.cc/Z4VY-T529>].

however, both countries moved toward strengthening the institutional autonomy of their authorities in order to align more closely with international standards.

In Argentina, Congress enacted the country's data privacy law in 2000, but the Executive Branch vetoed⁴⁶ the provision that would have established an independent supervisory authority, and instead created the authority within the Ministry of Justice,⁴⁷ subordinated to a sub-secretariat at the level of a national directorate. In other words, the Executive effectively captured the authority and placed it at a very low tier in the administrative hierarchy.⁴⁸ That institutional arrangement was subsequently modified by Decree No. 899/2017, which transferred the supervisory function to the Access to Public Information Agency (*Agencia de Acceso a la Información Pública*, "AAIP"), the body that currently serves as Argentina's data protection authority.⁴⁹

Brazil's path toward an independent supervisory authority was faster. While the Brazilian LGPD was originally approved by Congress in August 2018, which provided for the Brazilian DPA's creation, the president vetoed its creation at that time.⁵⁰ After the

46. Decreto 995/2000, Nov. 2, 2000, B.O. 29510 (Arg.) (partially promulgating and vetoing provisions of Law No. 25,326, including paragraphs 2 and 3 of Article 29 governing the supervisory authority). The stated rationale for the partial veto set forth in the recitals of Decree No. 995/2000 was fiscal in nature. The Executive Branch reasoned that establishing the data protection supervisory authority as a decentralized agency would necessarily entail increased expenditures by the national government to fund its operations, that the enabling legislation itself made no provision for the financing of such authority, and that neither the National Budget Law for fiscal year 2000 (Law No. 25,237) nor the proposed budget for fiscal year 2001 included appropriations to cover those costs. The decree further invoked the general principle of public financial administration law requiring that any increase in government expenditures be accompanied by a corresponding funding source. *Id.*

47. Decreto Reglamentario 1558/2001, anexo I, art. 29, Dec. 3, 2001, B.O. 29787 (Arg.).

48. Decreto Reglamentario 1558/2001 established the National Directorate for Personal Data Protection (*Dirección Nacional de Protección de Datos Personales*) within the orbit of the Secretariat of Justice and Legislative Affairs of the Ministry of Justice and Human Rights, designating it as the enforcement authority under Law No. 25,326 pursuant to Annex I, Article 29 of that decree. *See id.*

49. Decreto 899/2017, art. 1, Nov. 3, 2017, B.O. 33749 (Arg.) (substituting Article 29 of Annex I of Decree No. 1,558/2001 and vesting enforcement authority in the AAIP).

50. Mensagem No. 451, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.) (communicating President Michel Temer's partial veto of Law No. 13,709 (LGPD), which notably excised provisions creating the National Data Protection Authority (ANPD) due to unconstitutionality regarding executive initiative, as well as specific administrative sanctioning mechanisms).

veto, on December 28, 2018, the former president issued Provisional Measure No. 869, which re-created the Brazilian DPA and amended certain aspects of the LGPD.⁵¹ The veto occurred because the government did not want to create new expenses with a new authority; one of the major concerns was creating an independent agency.⁵² Thus, the National Data Protection Agency (“ANPD”) started as a government entity subordinate to the cabinet of the presidency, with no increased expenses. Several years later, a new government decided to issue Provisional Measure No. 1,317/2025⁵³ to transform the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*) into a full regulatory agency—the ANPD—endowed with administrative, functional, decisional, technical, and financial autonomy.⁵⁴

A parallel dynamic unfolded in El Salvador, where President Bukele vetoed a data protection law in May 2021 and its accompanying supervisory authority—both approved by the outgoing legislature—on grounds of alleged budgetary and constitutional inconvenience,⁵⁵ only to promote a tailor-made replacement three years later: The *Ley para la Protección de Datos Personales* and the *Ley de Ciberseguridad y Seguridad de la Información*, both approved on November 12, 2024, which vested data protection enforcement not in an independent authority, but

51. Medida Provisória No. 869, de 27 de Dezembro de 2018, Diário Oficial da União [D.O.U.] de 28.12.2018 (Braz.).

52. Lei No. 13.853, de 8 de Julho de 2019, Diário Oficial da União [D.O.U.] de 9.7.2019 (Braz.) (amending Lei No. 13.709/2018 (LGPD) to introduce arts. 55-A–55-L establishing the National Data Protection Authority (ANPD) with technical and decision-making autonomy).

53. Medida Provisória No. 1.317, de 17 de Setembro de 2025, Diário Oficial da União [D.O.U.] de 18.09.2025 (Braz.); Lei No. 15.221, de 29 de Setembro de 2025, Diário Oficial da União [D.O.U.] de 30.09.2025 (Braz.).

54. The actual measure enacted by the Brazilian government that transformed the ANPD into a special regime autarchy (regulatory agency)—endowed with technical, operational, administrative, and financial autonomy—was Provisional Measure No. 1,124/2022, promulgated on June 13, 2022, and subsequently enacted into Law No. 14,460/2022 on October 25, 2022.

55. See Diego Hernandez, *Bukele veta Ley de Protección de Datos Personales*, VOCES DIARIO DIG. (May 18, 2021), <https://voces.org.sv/bukele-veta-ley-de-proteccion-de-datos-personales/> [https://perma.cc/YP37-4K5M] (reporting the executive veto of the Ley de Protección de Datos Personales and the Ley de Creación de la Autoridad Nacional Digital, both approved by the Legislative Assembly on April 22, 2021, on grounds characterized as budgetary imbalance and lack of technical expertise).

in the newly created *Agencia de Ciberseguridad del Estado* (“ACE”), whose director is appointed directly by the President.⁵⁶

By contrast, in countries such as Colombia and Ecuador, the data protection function was incorporated into existing regulatory bodies—specifically, the superintendencies responsible for consumer protection and competition or intellectual property matters—reflecting a different institutional approach to enforcement in the region.⁵⁷

Even in Latin American jurisdictions lacking a formally designated data protection authority, the necessity of institutionalized data oversight became evident. For example, Chile’s data protection law, enacted in 1999, did not establish a specialized supervisory authority. The absence of such an authority led Chile’s consumer protection agency (“SERNAC”) to assume a quasi-regulatory role by issuing data protection guidance⁵⁸ and intervening in consumer disputes involving unsolicited commercial communications⁵⁹ and breaches of personal data.⁶⁰ This practice persisted until the comprehensive

56. Decreto Legislativo No. 144, *Ley para la Protección de Datos Personales*, Nov. 12, 2024 (El Sal.); see also *El Salvador: New Laws Threaten Free Expression, Privacy*, HUM. RTS. WATCH (Dec. 12, 2024), <https://www.hrw.org/news/2024/12/12/el-salvador-new-laws-threaten-free-expression-privacy> [<https://perma.cc/4BFL-CTZK>] (noting that the ACE’s director is a presidential appointee and that the agency’s broad “right to be forgotten” powers could be deployed to suppress critical journalism and public-interest information).

57. See L. 1581/2012, art. 19, octubre 17, 2012, *Diario Oficial* [D.O.] (Colom.) (designating the Superintendency of Industry and Commerce (Superintendencia de Industria y Comercio—SIC), through its Superintendency for Personal Data Protection, as the enforcement authority); *Ley Orgánica de Protección de Datos Personales*, art. 73, Mayo 26, 2021, *Registro Oficial* [R.O.] Sup. 459 (Ecuador) (establishing the Superintendency of Personal Data Protection (Superintendencia de Protección de Datos Personales) as the independent supervisory authority).

58. Servicio Nacional del Consumidor [SERNAC], *Circular Interpretativa Sobre Cláusulas Abusivas en Materia de Tratamiento de Datos Personales de los Consumidores*, Res. Exenta No. 138, Febrero 28, 2022 (Chile), <https://www.sernac.cl/portal/618/w3-article-65388.html> [<https://perma.cc/HM5U-3VHJ>] (establishing criteria regarding unfair contract terms in the collection and processing of consumers’ personal data under Law No. 19496 and Law No. 19628).

59. Law No. 19496, *Establece Normas Sobre Protección de los Derechos de los Consumidores*, art. 28 B, Marzo 7, 1997, *Diario Oficial* [D.O.] (Chile) (regulating unsolicited commercial communications sent to consumers and establishing opt-out rights).

60. See Lucas Del Villar, *El SERNAC y protección de datos*, SERNAC (June 23, 2021), <https://www.sernac.cl/portal/618/w3-article-62885.html> [<https://perma.cc/4GSD-RQ8E>] (discussing the complementary authority of Chile’s National Consumer Service to enforce personal data protection through collective actions and administrative proceedings within consumer relationships).

reform of the data protection framework in 2024, which expressly established an independent data protection authority.

Other jurisdictions, such as Costa Rica and Panama, have also established data protection authorities. However, these institutions often lack the stable funding and institutional capacity necessary to effectively carry out their supervisory and enforcement functions.

It is worth observing that the European model was not transposed in a pure or complete form with respect to the independence and autonomy of data protection authorities for a variety of reasons. These include chronic budget shortfalls, internal power struggles between the legislature and the executive branch (such as in Brazil and Argentina in their first years of enactment), and the frequent constitutional or administrative impossibility of establishing truly autonomous bodies of the kind that exist in Europe.

In practice, limited budgets and insufficient staffing have constrained their ability to oversee compliance and exercise their regulatory mandate in a manner comparable to more consolidated data protection regimes.

The following chart summarizes the main data protection authorities in the region and the year in which they were established:

Country	Year Created	Data Protection Authority
Argentina	2000	Agency for Access to Public Information (<i>Agencia de Acceso a la Información Pública – AAIP</i>)
Chile	2008	Council for Transparency (<i>Consejo para la Transparencia</i>) – supervisory functions regarding personal data in the public sector

Country	Year Created	Data Protection Authority
Uruguay	2009	Regulatory and Control Unit of Personal Data (<i>Unidad Reguladora y de Control de Datos Personales – URCDP</i>)
Colombia	2011	Superintendence of Industry and Commerce (<i>Superintendencia de Industria y Comercio – SIC</i>)
Peru	2011	National Authority for Personal Data Protection (<i>Autoridad Nacional de Protección de Datos Personales – ANPDP</i>)
Costa Rica	2011	Agency for the Protection of the Data of the Inhabitants (<i>PROD HAB</i>)
Mexico	2014	National Institute for Transparency, Access to Information and Personal Data Protection (<i>INAI</i>)
Panama	2019	National Authority for Transparency and Access to Information (<i>Autoridad Nacional de Transparencia y Acceso a la Información – ANTAI</i>)
Brazil	2020	National Data Protection Authority (<i>Autoridade Nacional de Proteção de Dados – ANPD</i>)
Ecuador	2021	Superintendence for the Protection of Personal Data (<i>Superintendencia de Protección de Datos Personales</i>)

3. Secondary Regulations of Privacy

In the field of data protection, the mere enactment of a statute is rarely sufficient to ensure the effective functioning of the regulatory framework. Comprehensive implementation requires the adoption of secondary legislation. It also demands the issuance of regulatory guidance. Such guidance must address a wide range of specific issues. These include security standards and sanctions regimes. International data transfer mechanisms must also be regulated. The appointment and duties of data protection officers require separate treatment. Additional compliance obligations round out the regulatory picture. Taken together, these measures are what give a data protection statute its practical effect.

In this field, the influence has been more selective, with data protection authorities importing specific GDPR concepts into their first-generation laws—such as the accountability principle in Colombia,⁶¹ data protection impact assessments,⁶² biometric data,⁶³ or the figure of the data protection officer⁶⁴ as well as

61. See Alejandro Bermudez Durana, *Accountability y protección de datos personales*, in 1 PROTECCIÓN DE DATOS PERSONALES: DOCTRINA Y JURISPRUDENCIA 367 (Pablo A. Palazzi ed., 2021).

62. The Argentine and Uruguayan DPAs jointly issued a data protection impact assessment guide. See Agencia de Acceso a la Información Pública [AAIP] & Unidad Reguladora y de Control de Datos Personales [URCDP], *Guía de Evaluación de Impacto en la Protección de Datos* (Jan. 28, 2020), https://www.argentina.gob.ar/sites/default/files/guia_final.pdf [<https://perma.cc/6DWH-XGU8>] [hereinafter *AAIP-URCDP DPIA Guide*].

63. See Agencia de Acceso a la Información Pública [AAIP], Resolución 4/2019, Jan. 13, 2019, B.O. No. 36.068, Anexo I, Criterio 4 (Arg.) (defining biometric data and declaring the criterion mandatory for all subjects covered by Law No. 25326); see also Agencia de Acceso a la Información Pública [AAIP], Resolución 255/2022, Dec. 15, 2022, B.O. No. 35.068 (Arg.) (extending equivalent sensitive-data classification to genetic data and reinforcing enhanced security, confidentiality, and access-restriction obligations for both biometric and genetic data under Law No. 25326, Article 9, and AAIP Resolution 47/2018).

64. See Unidad Reguladora y de Control de Datos Personales [URCDP], Resolución No. 32/020, May 19, 2020 (Uru.) [hereinafter *URCDP DPO Resolution 2020*] (clarifying qualification criteria for DPOs, establishing procedures for registration, and regulating DPOs that are legal entities rather than natural persons); see also Autoridade Nacional de Proteção de Dados [ANPD], Resolução CD/ANPD No. 18, de 16 de Julho de 2024, Regulamento sobre a atuação do Encarregado pelo Tratamento de Dados Pessoais, Diário Oficial da União [D.O.U.] de 17.07.2024 (Braz.) [hereinafter *ANPD DPO Regulation 2024*] (the principal regulatory instrument governing DPO appointment, functions, conflict of interest rules, and substitute designation requirements); Superintendencia de Protección de Datos Personales [SPDP], Resolución No. SPDP-SPD-2025-0028-R, *Reglamento del Delegado de Protección de Datos Personales*, July 30, 2025 (Ecuador) [hereinafter *SPDP DPO Regulation 2025*].

artificial intelligence (“AI”) guidelines⁶⁵ related to personal data into frameworks that otherwise retain significant structural differences from the European model.

At the same time, Latin American jurisdictions have not merely replicated some of the elements of the European model, but have also introduced new concepts that are not explicitly contemplated in the EU framework.

For instance, a Colombian scholar developed the notion of international data collection⁶⁶ (*recopilación internacional de datos personales*), a concept briefly mentioned in the regulation of the Colombian data privacy law⁶⁷ that has subsequently influenced regulatory developments in other jurisdictions, including Brazil in its recent regulations on international data transfer.⁶⁸ Moreover, the concept did not remain confined to national legislation. After emerging in Colombian law and later influencing regulatory developments in Brazil, the notion has also attracted attention at the international level. In particular, the United Nations Special Rapporteur on the right to privacy, Ana Brian Nougères, has taken up the idea and developed it extensively in a recent report⁶⁹ addressing contemporary challenges in cross-border data governance. This development illustrates how regulatory innovations originating in Latin America can themselves contribute to the broader evolution of global data protection norms.

65. See Superintendencia de Protección de Datos Personales [SPDP], Resolución No. SPDP-SPD-2026-0009-R, *Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial*, Feb. 12, 2026 (Ecuador) [hereinafter *SPDP AI Regulation 2026*]; see also Agencia de Acceso a la Información Pública [AAIP], *Guía para entidades públicas y privadas en materia de transparencia y protección de datos personales para una inteligencia artificial responsable* (July 2024), https://www.argentina.gob.ar/sites/default/files/guia_ai-final-2025.pdf [https://perma.cc/33KZ-MJ7D] [hereinafter *AAIP AI Guide (2025)*].

66. See NELSON REMOLINA ANGARITA, *RECOLECCIÓN INTERNACIONAL DE DATOS PERSONALES: UN RETO DEL MUNDO POST-INTERNET* (2015).

67. See L. 1581/2012, art. 21(j), octubre 17, 2012, *Diario Oficial* [D.O.] (Colom.); see also NELSON REMOLINA ANGARITA, *TRATAMIENTO DE DATOS PERSONALES: APROXIMACIÓN INTERNACIONAL Y COMENTARIOS A LA LEY 1581 DE 2012* 283 (2013).

68. See Resolução CD/ANPD No. 19, de 23 de Agosto de 2024, *Regulamento de Transferência Internacional de Dados Pessoais*, art. 6, *Diário Oficial da União* [D.O.U.] de 23.08.2024 (Braz.).

69. See Ana Brian Nougères (Special Rapporteur on the Right to Privacy), *Rep. of the Special Rapporteur on the Right to Privacy*, U.N. Doc. A/HRC/61/48 (2026), <https://docs.un.org/es/A/HRC/61/48> [https://perma.cc/9DMZ-FKMF].

In addition, certain jurisdictions have established a distinction between transfers (*transferencias*) and transmissions (*transmisiones*) of personal data,⁷⁰ using this distinction to differentiate situations in which data is shared with another controller from those in which data is merely processed by a service provider acting as a data processor.⁷¹ This conceptual differentiation made it more difficult to transplant the EU Standard Contractual Clauses⁷² models into these jurisdictions.

4. International Transfers of Personal Data in Latin America

In the specific domain of international transfers of personal data, Latin American jurisdictions have progressively incorporated into their domestic frameworks a set of transfer mechanisms closely modeled on their European counterparts.

Several countries in the region have adopted regulations governing Binding Corporate Rules,⁷³ Standard Contractual

70. See L. 1581/2012, arts. 3, 26–27, octubre 17, 2012, Diario Oficial [D.O.] (Colom.); see also Ley Orgánica de Protección de Datos Personales, arts. 70–72, Mayo 26, 2021, Registro Oficial [R.O.] Sup. 459 (Ecuador).

71. A controller is the natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data. A processor, by contrast, is a party that processes personal data on behalf of the controller, acting under the controller's instructions and without independent authority to determine the purposes of the processing. The distinction is significant because it allocates regulatory obligations and liability differently: controllers bear primary compliance responsibilities, while processors are subject to a more limited set of direct obligations, typically governed by a data processing agreement with the controller. See GDPR, *supra* note 12, arts. 4(7)–(8), 28.

72. Standard Contractual Clauses (SCCs) are pre-approved contractual templates issued by a data protection authority or competent regulatory body that establish adequate safeguards for the transfer of personal data to third countries that have not been recognized as providing an equivalent level of data protection. By incorporating SCCs into a data transfer agreement, the exporting party contractually binds the recipient to compliance obligations that mirror those applicable in the jurisdiction of origin, thereby providing a lawful basis for the transfer without the need for an individual authorization or adequacy determination. In the EU framework, SCCs are issued by the European Commission pursuant to Article 46(2)(c) of the GDPR and represent the most widely used mechanism for international data transfers in practice. Equivalent instruments exist in several Latin American jurisdictions. See GDPR, *supra* note 12, art. 46(2)(c).

73. See Agencia de Acceso a la Información Pública [AAIP], Resolución 159/2018, Lineamientos y Contenidos Básicos de Normas Corporativas Vinculantes, Dec. 7, 2018, B.O. (Arg.) (establishing the substantive guidelines and minimum content requirements for binding corporate rules as a mechanism for international personal data transfers from Argentina to countries lacking adequate protection, applicable to companies belonging to the same economic group); see also Decreto 255/2022, arts. 2.2.2.25.7.1–2.2.2.25.7.7, febrero 23, 2022, Diario Oficial [D.O.] (Colom.) [hereinafter *Decreto 255/2022*] (regulating

Clauses, and adequacy determinations and certification mechanisms, drawing heavily in both structure and substance on the guidelines, recommendations, and referential documents produced by the European Data Protection Board.⁷⁴

The influence of EDPB⁷⁵ guidance in this context has thus operated as a form of soft law transplantation,⁷⁶ shaping the

binding corporate rules as a transfer mechanism under L. 1581/2012, Article 27, requiring prior approval by the SIC; BCRs are mandatory and jointly enforceable against all members of the corporate group); Superintendencia de Protección de Datos Personales [SPDP], Resolución No. SPDP-SPD-2026-0004-R, Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales, arts. 20–34, Febrero 13, 2026 (Ecuador) [hereinafter *SPDP Transfer Regulation 2026*] (establishing binding corporate rules—normas corporativas vinculantes—as one of the recognized “adequate safeguards” for international data transfers to countries without an adequacy declaration, alongside standard contractual clauses, codes of conduct, and certification mechanisms; requiring SPDP prior approval of BCRs).

74. See European Data Protection Board, *Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR* (Nov. 18, 2021), https://www.edpb.europa.eu/documents/guideline/guidelines-052021-on-the-interplay-between-the-application-of-article-3-and-the_en [<https://perma.cc/EF26-QFM8>]; see also European Data Protection Board, *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (June 18, 2021); Red Iberoamericana de Protección de Datos (RIPD), *Estándares de Protección de Datos Personales para los Estados Iberoamericanos* (June 20, 2017), https://www.redipd.org/sites/default/files/2019-10/estandares_en.pdf [<https://perma.cc/W9LN-9NKH>].

75. The European Data Protection Board (EDPB) is an independent body established under Article 68 of the GDPR, composed of the heads of the national supervisory authorities of each EU Member State and the European Data Protection Supervisor. The EDPB is responsible for ensuring the consistent application of the GDPR across the European Union, issuing binding decisions in cross-border cases, and adopting guidelines, recommendations, and best practices on a wide range of data protection matters. Although its instruments are formally addressed to EU Member States and their supervisory authorities, the EDPB’s guidelines have acquired significant influence beyond European borders, functioning in practice as a primary source of soft law reference for data protection regulators and legislators worldwide, including in Latin America.

76. The concept of soft law transplantation, as used here, refers to the voluntary adoption by Latin American regulators and legislators of non-binding instruments—such as guidelines, recommendations, working party opinions, and regulatory frameworks—developed primarily within the European data protection ecosystem. Unlike hard law transplantation, which involves the incorporation of binding legal obligations through treaties, statutes, or formally enacted secondary legislation, soft law transplantation operates through persuasion, institutional emulation, and regulatory convergence rather than legal compulsion. The adopting jurisdiction is under no obligation to incorporate these instruments, yet chooses to do so—whether for reasons of regulatory legitimacy, technical capacity, cross-border interoperability, or alignment with trading partners. This distinction is analytically significant because it reveals that the Europeanization of Latin American data protection law is not solely a product of formal legal diffusion, but also of a

technical content of Latin American transfer regulations in ways that the Brussels Effect alone—understood primarily as a market-driven phenomenon—does not fully capture.⁷⁷

The best example is the SCC model⁷⁸ drafted by the RIPD⁷⁹ following the EU Model Contractual Clauses (“MCCs”) that the European Commission drafted in 2021.⁸⁰ Already six countries in the region have approved these SCCs in their respective jurisdictions.⁸¹

The swift uptake of the RIPD’s SCCs adopted by Peru, Uruguay, Argentina, Chile, Colombia, and Ecuador as the operative standard for international transfers signals something important: The RIPD has established itself as the source of regional standard-setting via soft law.⁸²

In 2024, Brazil enacted the ANPD Resolution on international data transfers,⁸³ which established procedures and rules

quieter, voluntary process by which soft European standards are gradually hardened into local regulatory practice.

77. See BRADFORD, *supra* note 6, at 126–52; see also Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 795–800 (2019).

78. Red Iberoamericana de Protección de Datos, *supra* note 37.

79. The Ibero-American Data Protection Network (Red Iberoamericana de Protección de Datos, RIPD) is a multilateral forum composed of data protection authorities and government bodies from Spain, Portugal, and Latin American countries, established to promote cooperation, harmonization, and the development of common data protection standards across the Ibero-American region. The RIPD serves as a key institutional venue for the exchange of regulatory experience and the elaboration of shared frameworks, including model laws and joint declarations. While its instruments are non-binding, the RIPD has functioned as an important soft law producer within the region, influencing both legislative reform and regulatory practice in member jurisdictions. It has also served as a bridge between the European data protection tradition and Latin American legal systems, facilitating the adaptation of GDPR-aligned concepts to the specific legal and institutional contexts of the region.

80. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679, 2021 O.J. (L 199) 31.

81. See PABLO A. PALAZZI, CONTRATO DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES 286, 289 (2026) (listing Latin American countries that adopted internally the RIPD SCC).

82. This harmonizing potential must be understood against an important institutional constraint: the RIPD is not a supranational regulator. Unlike the EDPB—which can issue binding decisions enforceable across the European Union—the RIPD has no authority to impose obligations on member states, national authorities, or private parties. Every instrument it produces is soft law, and its normative reach extends only as far as national lawmakers and data protection authorities are willing to carry it. The Network’s credibility is earned, not mandated.

83. See Resolução CD/ANPD No. 19, *supra* note 68.

applicable to the international transfer of personal data, in accordance with the provisions of the LGPD and the Internal Regulations of the ANPD, aiming to ensure safe and transparent international transfers of personal data.

In December 2025, the Colombian data protection authority approved its regulation⁸⁴ on SCCs, drawing on the RIPD model and including a series of practical guidance provisions on how to implement the clauses in practice. The regulation closely follows the European Commission's FAQ on the EU standard contractual clauses, reflecting a deliberate alignment with the European approach to contractual transfer mechanisms.⁸⁵

In January 2026, the Ecuadorian data protection authority regulated international data transfers,⁸⁶ adopting definitions of international transfer closely aligned with the European model. The Resolution established an adequacy determination process and a corresponding procedure. The Resolution also approved the RIPD standard contractual clauses, binding corporate rules, codes of conduct, and certifications as valid transfer mechanisms, following the GDPR framework in considerable detail. The Resolution went even further by introducing a presumption of validity for international data transfers between member states of the Andean Community of Nations.⁸⁷

A further manifestation of the Brussels Effect in Latin American standard contractual clause frameworks is the influence of the reasoning underlying *Schrems II*. That decision fundamentally recast the role of data exporters and importers, imposing on them an active due diligence obligation with respect

84. Superintendencia de Industria y Comercio [SIC], Resolución No. 3/2025 (Colom.).

85. The relevant provisions of Colombian data protection regulation were not derived from the binding text of the EU's Standard Contractual Clauses themselves, but rather from the FAQ documents published by European authorities to guide their interpretation and practical implementation.

86. See *SPDP Transfer Regulation 2026*, *supra* note 73.

87. The Andean Community of Nations (Comunidad Andina de Naciones, CAN) is a regional trade and integration bloc comprising Bolivia, Colombia, Ecuador, and Peru. Founded in 1969 under the Cartagena Agreement, it is one of the oldest regional integration frameworks in Latin America, encompassing a common external tariff, harmonized trade rules, and a supranational legal order through the Andean Court of Justice. The presumption of validity for intra-CAN data transfers introduced by Ecuador's Resolution 4-2026 draws on this pre-existing framework of regional legal integration, treating member states as a zone of equivalent regulatory trust—a logic not unlike the EU's internal market approach to personal data flows.

to government access requests in the recipient country. Rather than treating the execution of standard contractual clauses as a self-sufficient compliance mechanism, *Schrems II* requires parties to assess, on a case-by-case basis, whether the legal order of the destination country provides adequate protection in practice—and to adopt supplementary measures where it does not. This shift from passive reliance to active responsibility has reverberated beyond the European Union, shaping the design of SCC frameworks in Latin American jurisdictions that have sought alignment with the post-*Schrems II* standard.

That logic was transposed into the standard contractual clauses adopted by Brazil and into the model clauses developed under the Ibero-American Data Protection Network, which several Latin American countries have already adopted.⁸⁸ Both SCC models require the data importer to assess the legality of any disclosure request, including whether it falls within the powers of the requesting public authority. The SCC models also require the parties of the SCC to challenge the request if, upon careful assessment, there are reasonable grounds to conclude that it is unlawful under the laws of the destination country, applicable international law obligations, or principles of international comity.⁸⁹

The convergence of Latin American data protection frameworks around the European model—through the adoption of standard contractual clauses and adequacy country lists—represents not mere regulatory mimicry, but a deliberate and structurally coherent strategy that closes the circle: By internalizing the very instruments on which the EU conditions cross-border data transfers, Latin American jurisdictions simultaneously secure their eligibility as adequate or equivalent destinations under European law, and erect, within their own legal orders, the same protective barriers against onward transfers to third countries that do not meet equivalent standards.

But the circle may not remain closed for long: US-driven, unilateral “adequacy” recognitions embedded in trade agreements

88. See PALAZZI, *supra* note 81, at 356 (explaining how the doctrine of *Schrems II* was transplanted into the RIPD SCC clauses).

89. See Case C-311/18, Data Prot. Comm’r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020); see also LGPD art. 33 (Braz.).

threaten to puncture these EU-modeled barriers, as shown in Section III.B of this Article.

5. Adequacy Determinations of Latin American Countries

The influence of the European Union's data protection framework in Latin America is observable through the adoption of adequacy decisions recognizing certain jurisdictions as providing a level of protection essentially equivalent to that of the European Union.

Countries in the region have a strong incentive to obtain such recognition, as adequacy allows the free flow of personal data and related services to Europe without the need for additional transfer mechanisms. Indeed, policymakers in several jurisdictions have openly acknowledged that one of the motivations behind adopting or reforming data protection legislation is precisely to obtain EU adequacy status.⁹⁰

For jurisdictions that secured EU adequacy recognition under the pre-GDPR framework—which includes Argentina in 2003 and Uruguay in 2012—the maintenance of that status has become an independent driver of legislative reform.⁹¹ Adequacy decisions are subject to periodic review, and as the GDPR has replaced the 1995 Directive as the operative benchmark, the level of protection required to sustain recognition has risen considerably.⁹² Countries holding adequacy status thus face a standing incentive not merely to preserve their existing frameworks, but to update them in line with GDPR standards—lest a future review conclude that their domestic law no longer meets the threshold of essential equivalence.

90. Arturo J. Carrillo & Matías Jackson, *Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, 16 VIENNA J. INT'L CONST. L. 177 (2022).

91. In the case of Uruguay, these reforms have been recursive, occurring at regular intervals as noted above. In the case of Argentina, several legislative bills have been introduced to update the existing framework in line with the GDPR, as discussed above, but none has been enacted, owing to persistent legislative inertia.

92. The GDPR provides that adequacy decisions adopted prior to its entry into force would remain valid but would be subject to periodic review. In particular, the Regulation establishes that such decisions must be monitored on an ongoing basis and reviewed at least every four years to assess whether the third country continues to ensure an adequate level of protection. See GDPR, *supra* note 12, art. 45(3)–(4).

At the same time, the model of adequacy itself has evolved. In the first two cases—Argentina and Uruguay—the recognition was a unilateral decision adopted by the European Union.⁹³ By contrast, in the case of Brazil, the adequacy framework took the form of a bilateral recognition, reflecting a more reciprocal approach to cross-border data governance.

The following table summarizes, in chronological order, the Latin American countries that have obtained such recognition from the European Union.

Country	Year	Comment
Argentina	2003	The European Commission recognized Argentina as providing an adequate level of protection for personal data under its Personal Data Protection Act (Law No. 25,326), allowing personal data to flow from the European Union to Argentina without the need for additional transfer safeguards. The adequacy finding was subsequently revalidated under the GDPR in 2024.
Uruguay	2012	The European Commission determined that Uruguay ensures an adequate level of protection for personal data under its Personal Data Protection Act (Law No. 18,331), enabling transfers of personal data from the EU without additional transfer mechanisms. The adequacy finding was subsequently revalidated under the GDPR in 2024.

93. Commission Decision 2003/490/EC of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, 2003 O.J. (L 168) 19; Commission Implementing Decision 2012/484/EU of 21 August 2012 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Eastern Republic of Uruguay with Regard to Automated Processing of Personal Data, 2012 O.J. (L 227) 11.

Country	Year	Comment
Brazil	2026	On January 27, 2026, the EU and Brazil adopted <i>mutual adequacy decisions</i> establishing a trusted data corridor between the two jurisdictions.

Despite the strong global influence of the EU's data protection model, the number of adequacy recognitions in Latin America has remained limited. Over roughly twenty-five years, the European Union has granted adequacy status to only three countries in the region—Argentina, Uruguay, and Brazil—leaving outside major economies such as Colombia, Peru, and Mexico. This limited expansion has prompted criticism from some scholars, including Professor Nelson Remolina,⁹⁴ who argued that the EU's adequacy process has been slow and insufficiently responsive to regulatory developments in Latin America.

By contrast, the United States has moved quickly to build trusted data ties in the region: In less than a year, the United States secured multiple unilateral US-adequacy recognitions for cross-border data flows through trade-based agreements—an approach examined in Section III.B of this Article.

III. THE “WASHINGTON EFFECT”: THE REGULATORY ALIGNMENT THROUGH TRADE AGREEMENTS

A. The United States' Position on International Data Flows

The United States sits uneasily in the global data-protection order. Unlike the European Union's unitary, rights-based framework, US privacy regulation remains largely sectoral—a patchwork of federal statutes, state laws,⁹⁵ and enforcement anchored in consumer-protection authority rather than a

94. See Nelson Remolina, *Is It Worthwhile for Latin American Countries to Obtain Adequate Level of Personal Data Protection from the European Approach, or Is It Better to Promote the Use of Contractual Clauses to Export Such Information?*, 10 UNIO EU L.J. 71 (2024).

95. See JOEL R. REIDENBERG & PAUL SCHWARTZ, DATA PRIVACY LAW 129 (1996).

comprehensive data-protection federal law.⁹⁶ In practice, the Federal Trade Commission has functioned as the *de facto* national privacy enforcer⁹⁷ by policing “unfair or deceptive” practices, and turning privacy commitments into enforceable obligations⁹⁸ across much of the data economy.

That institutional reality also explains what the United States generally does not do. It has not adopted a GDPR-style architecture of *ex ante* obligations (for example, universal legal bases, systematic privacy impact assessments, mandatory DPO requirements, or across-the-board limits on sensitive-data processing), nor has it built an EU-type transfer regime that conditions cross-border flows on “adequacy” determinations or standardized safeguards like SCCs as a legal precondition. From the United States’ perspective, imposing such contractual requirements on local companies could be seen as inconsistent with principles favoring open markets and the free flow of commerce, except for national security purposes.⁹⁹ The default posture has instead favored free flows of information, with constraints framed primarily through national security and narrow sectoral rules.

This divergence has produced predictable transatlantic friction. EU courts have repeatedly invalidated EU–US transfer arrangements (Safe Harbor and Privacy Shield), reflecting the EU’s constitutional commitment to data protection as a fundamental

96. Woodrow Hartzog & Neil Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1690–92 (2020) (observing that the United States lacks a general federal data protection law and instead relies on a patchwork of sectoral legislation and FTC enforcement authority under Section 5 of the FTC Act).

97. See CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); see also Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

98. See Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305 (2001).

99. US regulators are increasingly treating cross-border data transfers to foreign adversaries as a national security issue, signaling a shift toward stricter federal and state oversight following the enactment of the Protecting Americans’ Data from Foreign Adversaries Act (PADFAA) and related regulatory initiatives. See Protecting Americans’ Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I, 138 Stat. 895, 960.

right,¹⁰⁰ and the resulting willingness to strike down frameworks perceived as incompatible with that standard.¹⁰¹

Beyond this domestic regulatory landscape, the United States has historically advocated internationally for the principle of the free flow of information and has generally opposed strict regulatory constraints on cross-border data flows.¹⁰² In trade negotiations and international digital policy discussions, US policy has consistently favored frameworks that facilitate the unrestricted movement of data across borders, viewing such flows as essential to global commerce, innovation, and the functioning of the digital economy.¹⁰³

At the same time, the United States' "free flow" posture has become more assertive in diplomatic practice, including internal instructions to resist data-sovereignty and localization initiatives abroad, and to promote CBPR-style alternatives.¹⁰⁴

In Latin America, the United States has leveraged trade policy as its main governance vehicle for data flows. Modern trade

100. See Charter of Fundamental Rights of the European Union arts. 7–8, 2012 O.J. (C 326) 391.

101. See PALAZZI, *supra* note 81, at 167–71 (arguing that the Charter of Fundamental Rights of the European Union, as interpreted by the Court of Justice of the European Union in a long line of cases, has become a central constitutional instrument for defining the scope and content of the right to personal data protection—with significant consequences, among others, for the legal regime governing the international transfer of personal data). The Safe Harbor Agreement and the Privacy Shield framework constitute the two successive transatlantic data transfer mechanisms invalidated by the Court of Justice of the European Union in *Schrems I* and *Schrems II*, respectively.

102. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 128 (2017) ("Unlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action.").

103. See Priscilla M. Regan, *American Business and the European Data Protection Directive: Lobbying Strategies and Tactics*, in VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 199 (Colin J. Bennett & Rebecca Grant eds., 1999).

104. See Raphael Satter & Alexandra Alper, *US Orders Diplomats to Fight Data Sovereignty Initiatives*, REUTERS (Feb. 25, 2026), <https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25/>, [https://perma.cc/4XKQ-84VC]. In February 2026, the US State Department issued an internal diplomatic cable signed by Secretary of State Marco Rubio, directing US diplomats worldwide to lobby against data sovereignty and data localization initiatives abroad, on the grounds that such measures disrupt global data flows, raise costs, limit AI and cloud services, and risk enabling government censorship. The cable explicitly singled out the EU's GDPR as an example of "unnecessarily burdensome data processing restrictions," and tasked diplomats with promoting the Global Cross-Border Privacy Rules (CBPR) Forum as an alternative multilateral framework. *Id.*

instruments embed pro-flow disciplines—most visibly the United States–Mexico–Canada Agreement’s (“USMCA”) digital trade chapter (cross-border data flow commitments, limits on localization requirements, and constraints on source-code disclosure), alongside encouragement of interoperability mechanisms such as CBPR.

The practical consequence is a normative ratchet. By locking “free flow” commitments into binding trade obligations, the United States can narrow partners’ regulatory space for Brussels-style transfer conditionality. And at the same time, the United States is still securing “adequacy-like” outcomes through trade diplomacy—illustrated by Argentina’s commitment, in the US–Argentina reciprocal trade framework, to recognize the United States as an “adequate jurisdiction” for cross-border data transfers, including personal data.

B. Unilateral Recognition of Adequacy of the United States in Trade Agreements

International trade agreements come in different forms. The most comprehensive are free trade agreements, which typically address tariffs, market access, investment, intellectual property, and an increasingly broad range of regulatory matters, including digital trade and data flows.¹⁰⁵ A narrower but still significant instrument is the bilateral investment treaty, which focuses on the conditions and protections applicable to foreign investment between two states.¹⁰⁶ Most recently, the United States introduced a new and distinct instrument, the Agreement on Reciprocal Trade (“ART”), which was designed to address specific trade imbalances and non-tariff barriers through targeted bilateral commitments that fall short of a comprehensive free trade agreement in scope,

105. Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT’L L. 407, 410–14 (2017) (observing that contemporary free trade agreements have evolved into comprehensive regulatory instruments addressing not only tariffs and market access but also investment, intellectual property, and an expanding array of digital trade issues including cross-border data flows).

106. Kenneth J. Vandeveld, *A Brief History of International Investment Agreements*, 12 U.C. DAVIS J. INT’L L. & POL’Y 157, 158–61 (2005) (distinguishing bilateral investment treaties, which focus exclusively on investment protection standards such as fair and equitable treatment and expropriation, from free trade agreements, which address a broader range of trade-related obligations including tariffs, services, and market access).

but exceed a mere tariff schedule in normative ambition. It is this last category that is of particular relevance to the present analysis.

During 2025 and 2026, the United States signed Agreements on Reciprocal Trade with four Latin American countries: Argentina,¹⁰⁷ Ecuador,¹⁰⁸ El Salvador,¹⁰⁹ and Guatemala.¹¹⁰ Each of these instruments contains provisions on digital trade and cross-border data flows that, taken together, constitute the most concrete recent expression of the Washington Effect in the region and provide the empirical foundation for the argument developed in the sections that follow.

These agreements regulate personal data in cross-border digital trade. That is familiar territory.¹¹¹ However, the twist is that they translate cross-border transfer doctrine—including US “adequacy”—into trade commitments; and in some cases, pair that move with the APEC CBPR as an operative transfer tool rather than leaving it as abstract language.

For example, the provision of digital trade and data requires Argentina to recognize the United States as an adequate partner for the purposes of facilitating the free flow of data¹¹² and commit the parties to promote interoperability mechanisms for international data transfers, including the use of certification-based

107. United States of America – Argentine Republic Agreement on Reciprocal Trade and Investment, U.S.-Arg., Feb. 5, 2026, <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf> [<https://perma.cc/5D9F-GLL7>] [hereinafter *US–Argentina Agreement*].

108. Agreement Between the United States of America and the Republic of Ecuador on Reciprocal Trade, U.S.-Ecuador, Mar. 13, 2026, Office of the U.S. Trade Representative.

109. Agreement Between the United States of America and the Republic of El Salvador on Reciprocal Trade, U.S.-El Sal., Jan. 29, 2026, Office of the U.S. Trade Representative.

110. Agreement Between the United States of America and the Republic of Guatemala on Reciprocal Trade, U.S.-Guat., Jan. 30, 2026, Office of the U.S. Trade Representative.

111. See Mira Burri, *Creating Data Flow Rules through Preferential Trade Agreements*, in DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 264–92 (Anupam Chander & Haochen Sun eds., 2023) (identifying early and later PTAs containing privacy/data-protection language in digital trade, including the Jordan–U.S. FTA (2000), the Canada–Costa Rica FTA (2001), and the USMCA).

112. See US–Argentina Agreement, *supra* note 107, at 34 (“Argentina shall provide certainty regarding the ability to move personal data out of its territory to the United States including by recognizing the United States as a country or jurisdiction that provides adequate data protection under Argentina’s law.”).

frameworks,¹¹³ such as the APEC Cross-Border Privacy Rules system and to integrate the Global Cooperation Arrangement for Privacy Enforcement.¹¹⁴

The wording of the unilateral adequacy recognition varies across instruments. In some cases, it is framed expressly as “recognizing the United States as an adequate jurisdiction” for cross-border transfers of data (including personal data), while other texts include a deadline for the recognition:

Country	Text of the adequacy recognition
Argentina	Argentina shall provide certainty regarding the ability to move personal data out of its territory to the United States including by recognizing the United States as a country or jurisdiction that provides adequate data protection under Argentina’s law.
Ecuador	Ecuador shall provide certainty regarding the ability to move personal data outside of its territory to the United States and shall endeavor to recognize the United States as a country or jurisdiction that provides adequate data protection under its legal framework by December 31, 2026.
Guatemala	Guatemala shall provide certainty regarding the ability to move personal data out of its territory to the United States, including by recognizing the United States as a country or jurisdiction that provides adequate data protection under Guatemala’s law.

113. *See id.* (“Argentina shall submit its letter of intent to participate as an Associate in the Global Cross-Border Privacy Rules Forum and to participate in the Global Cooperation Arrangement for Privacy Enforcement.”).

114. The Global Cooperation Arrangement for Privacy Enforcement (Global CAPE) is a non-binding, multilateral, voluntary framework allowing privacy enforcement authorities (PEAs) to collaborate on cross-border data protection issues. Established by the Global CBPR Forum, it helps members share information, conduct investigations, and render assistance to enforce privacy laws across borders.

Country	Text of the adequacy recognition
El Salvador	El Salvador shall consider the United States as a country that has an adequate data protection standard for the purpose of transferring personal data across borders under its law.

These negotiations reflected a broader US policy objective: To promote the free flow of information across borders and to embed data governance principles within trade frameworks rather than within comprehensive privacy legislation. The USMCA's announced review¹¹⁵ in 2026 may well follow the same path, amending the agreement to further include similar "trusted data" commitments with Canada and Mexico.

The emergence of unilateral adequacy recognition mechanisms in trade agreements concluded by the United States gives rise to two important observations. First, the very use of the concept of "adequacy" by the United States reflects the normative influence of European data protection law.¹¹⁶ The notion of adequacy was originally developed by local European laws in the 1980s and then by the European Union in the 1995 Data Protection Directive as a mechanism to regulate international transfers of personal data by ensuring that third countries provide a level of protection essentially equivalent to that guaranteed within the European Union.¹¹⁷ The incorporation of adequacy-like recognition clauses in US trade instruments can therefore be understood, at least implicitly, as an acknowledgment that the concept has become a relevant regulatory benchmark in the

115. *US Begins Review of Trade Deal with Canada and Mexico*, FIN. TIMES (Sept. 16, 2025), <https://www.ft.com/content/8bd947d1-3616-4c01-9674-605bc950dddd> [<https://perma.cc/C479-P39U>] (reporting that Washington opened a public comment period for businesses ahead of a possible renegotiation of the USMCA).

116. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 1995 O.J. (L 281) 31 (establishing the concept of "adequate protection" as the standard for transfers of personal data to third countries); GDPR, *supra* note 12, art. 45 (retaining and elaborating the adequacy standard, authorizing the European Commission to determine by decision whether a third country ensures an adequate level of protection).

117. See CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 26 (2013).

governance of cross-border data flows. In that sense, the diffusion of the adequacy framework beyond the European regulatory sphere may be viewed as a success of the European Union's normative project in shaping the global vocabulary of data protection.

At the same time, however, the emergence of parallel recognition mechanisms led by the United States may gradually erode the coherence and authority of the adequacy regime as originally conceived by the European Union. The EU adequacy determination process is highly structured, involving a detailed assessment¹¹⁸ of a third country's legal framework, institutional safeguards, enforcement mechanisms, and respect for fundamental rights.¹¹⁹

By contrast, adequacy-like recognition under trade agreements may operate through political or diplomatic channels that do not replicate the same procedural rigor or substantive benchmarks. The existence of an alternative pathway for international data transfer recognition—one that may require fewer institutional steps than the European adequacy process—introduces a competing regulatory model grounded in a different legal and policy philosophy.

Over time, this divergence between the European and US approaches could contribute to a fragmentation of the adequacy concept itself. Rather than functioning as a singular and highly standardized benchmark for cross-border data protection, adequacy may evolve into a plural and contested notion, interpreted differently across regulatory regimes. In this scenario, the very success of the European Union in disseminating the language of adequacy may paradoxically weaken the clarity and uniformity of the concept, as other actors adapt and reshape it within alternative legal frameworks.

Here the reader may recall Chander and Schwartz's influential account of the "splintering" of the adequacy principle, by which the once unitary EU concept has fragmented as it diffuses across jurisdictions lacking a common substantive definition or

118. See Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, DG XV D/5025/98 WP 12 (Jan. 24, 2002).

119. See GDPR, *supra* note 12, art. 45.

procedural discipline.¹²⁰ Their diagnosis is descriptively accurate insofar as multiple nations around the world today deploy the vocabulary of “adequacy” to pursue heterogeneous regulatory agendas. Yet this fragmentation should not obscure a crucial distinction between the EU-original adequacy term and the new trade-based adequacy emerging from the US-led digital trade agreements. The former is anchored in a rights-based architecture that empowers public authorities to block data flows absent a comprehensive assessment of a third country’s legal framework, individual rights, institutional safeguards, and effective remedies—which is now codified in Article 45 GDPR.¹²¹ The latter, by contrast, operationalizes “adequacy” as a functional trade instrument—decoupled from constitutional rights review and oriented toward facilitating data flows. What appears at first glance as mere splintering thus masks a deeper bifurcation: Not simply multiple national interpretations of a shared concept, but two competing paradigms of adequacy itself—one grounded in fundamental rights and regulatory veto power, the other in market access and trade liberalization.¹²²

On the other hand, this institutional and procedural complexity also helps explain why, in more recent cases, the European Union has increasingly relied on bilateral adequacy processes. Rather than conducting a purely unilateral assessment of a third country’s legal framework, the European Commission has in certain instances engaged in structured bilateral negotiations aimed at aligning specific aspects of the third country’s legal regime with European data protection standards.

The adequacy decision adopted with respect to Japan¹²³ illustrates this approach, where regulatory adjustments and mutual understandings were developed through a coordinated

120. See Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49 (2023).

121. See GDPR, *supra* note 12, art. 45.

122. Svetlana Yakovleva & Kristina Irion, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU’s International Trade “Deals”?*, 16 WORLD TRADE REV. S71, S73–75 (2017) (warning that the economic approach to privacy supported by trade institutions risks displacing the fundamental rights framework through the back door of trade liberalization commitments).

123. See Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information, 2019 O.J. (L 76) 1 [hereinafter *EU–Japan Adequacy Decision*].

dialogue between the European Commission and the Japanese authorities.¹²⁴ A similar dynamic is observed in the discussions surrounding Brazil's data protection framework.¹²⁵ These developments suggest a gradual evolution of the adequacy mechanism from a strictly unilateral evaluation toward a more cooperative and negotiated process of regulatory convergence.

C. The Alternative of Piggybacking on the Existing EU-US Adequacy Agreements or EU Adequacy Determinations

A further strategic option available to Latin American states—one that has received insufficient attention in the comparative literature—is what might be termed regulatory piggybacking on either the existing transatlantic adequacy framework or on the EU's adequacy determinations.

For example, a Latin American state may negotiate a bilateral adequacy decision with the European Commission that explicitly incorporates the Data Privacy Framework ("DPF") redress and oversight mechanisms as a benchmark, thereby free-riding on the political and legal capital that Washington invested in obtaining its own adequacy-equivalent status from Brussels. To date, that path remains purely hypothetical: The European Commission's DPF adequacy decision is a bespoke EU-US instrument limited to US organizations participating in the DPF.¹²⁶

The second modality is structurally simpler but legally more autonomous: A country internally adopts as its own the EU's list of adequate countries, so that personal data may flow freely to any jurisdiction that the European Commission has already recognized as adequate, without the Latin American state independently conducting its own assessment.

124. *EU-Japan Adequacy Decision*, *supra* note 123.

125. On January 26–27, 2026, the European Commission and Brazil formally adopted mutual adequacy decisions, recognizing each other's data protection regimes (GDPR and LGPD) as providing an equivalent level of protection. The EU recognized Brazil's LGPD, and Brazil (via ANPD Resolution No. 32) recognized the EU, enabling seamless, two-way data transfers.

126. Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118 (establishing a bilateral framework for international data transfers exclusively between the United States and the European Union).

In this case, rather than conducting an independent and comprehensive evaluation of a third country's data protection regime, some jurisdictions have effectively relied on the adequacy analysis already undertaken by the European institutions, thereby replicating or "cloning" the adequacy assessment performed by the EU.¹²⁷ In such scenarios, the country in question, instead of carrying out its own assessment or negotiating a separate framework, effectively "hooks into" the system negotiated between the EU and the United States, and approves US companies that have self-certified under the EU-US framework solely upon proof that such registration has taken place.

Countries such as Uruguay,¹²⁸ for instance, have adopted mechanisms¹²⁹ that directly or indirectly rely on the EU's assessment when determining whether certain international data transfer arrangements provide sufficient safeguards.¹³⁰ In practice, this has sometimes taken the form of recognizing transfers to the

127. The rationale underlying this approach is relatively straightforward: If the European Union has determined that a particular jurisdiction—such as the United States—provides an adequate level of protection through a specific legal arrangement, a third country may reasonably rely on that determination as persuasive authority for its own recognition of adequacy. In other words, once the European Union has conducted the extensive legal and institutional analysis required to conclude that a given framework satisfies the adequacy standard, other jurisdictions may consider that assessment sufficiently robust to justify adopting a similar conclusion within their own legal systems. From this perspective, the EU's adequacy decision operates not only as a regulatory instrument governing data transfers from the European Union, but also as a *de facto* benchmark capable of informing and shaping the adequacy determinations of third countries.

128. Uruguay recognizes the United States as having an adequate level of data protection, specifically for organizations certified under the EU-US Data Privacy Framework (DPF). In November 2023, Uruguay's regulatory authority (URCDP) updated its list of adequate countries to include certified US entities, that is, entities that joined the DPF. *See* Unidad Reguladora y de Control de Datos Personales [URCDP], Resolución No. 63/023, Nov. 21, 2023 (Uru.).

129. *See* Unidad Reguladora y de Control de Datos Personales [URCDP], Resolución No. 23/021, June 8, 2021 (Uru.); *see also* URCDP, Resolución No. 63/023, Nov. 21, 2023 (Uru.); URCDP, Resolución No. 70/023, Complementar lo establecido por las Resoluciones N° 23/021, de 8 de junio de 2021 y N° 63/023, de 22 de noviembre de 2023 (Uru.).

130. Unidad Reguladora y de Control de Datos Personales [URCDP], Resolución No. 63/023, Nov. 21, 2023 (Uru.), <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023> [<https://perma.cc/478H-S339>] (recognizing organizations certified under the EU-US Data Privacy Framework as adequate destinations for international transfers of personal data from Uruguay).

United States through mechanisms that mirror or depend upon the EU-US data transfer frameworks.¹³¹

Argentina offers the clearest illustration of regulatory piggybacking in practice. In November 2016, the then Argentine DPA (Dirección Nacional de Protección de Datos Personales, “DNPDP”) issued a decision¹³² which simultaneously adopted standard contractual clauses for international data transfers, and also published a list of countries deemed to provide an adequate level of protection for purposes of its data protection law. The decision drew explicitly on the experience of the Article 29 Working Party¹³³ and determined that it was convenient to identify those countries that, in the DNPDP’s judgment,¹³⁴ possessed adequate legislation, a list that, at the time of its adoption, was coextensive with the countries that the European Commission had individually recognized as adequate under Directive 95/46/EC. With this decision, the DPA of Argentina was operationalizing, in Argentine law, the first modality of adequacy piggybacking described above. The Brussels Effect could not have found a more direct domestic expression: Argentina’s adequacy map was, for all practical purposes, a clone of the EU’s own list.¹³⁵

131. See *The Data Protection Agency of Uruguay Includes the United States Amongst Safe Countries for International Data Transfers*, ALLENDE & BREA (Nov. 27, 2023), <https://allende.com/en/privacy-and-cybersecurity/the-data-protection-agency-of-uruguay-includes-the-united-states-among-countries-eligible-for-international-transfers-11-27-2023> [https://perma.cc/ASG5-PMHU].

132. See Dirección Nacional de Protección de Datos Personales [DNPDP], Disposición 60-E/2016, Nov. 16, 2016, B.O. (Arg.) (approving standard contractual clauses for international personal data transfers and establishing the list of countries deemed to provide adequate protection under Law No. 25326).

133. The Article 29 Working Party (established under Article 29 of Directive 95/46/EC) was the predecessor advisory body to the European Data Protection Board, which replaced it upon the entry into force of the GDPR in May 2018. See *GDPR*, *supra* note 12, art. 94(2).

134. Argentina’s data protection authority opened an internal case file in which each candidate country was independently assessed; the resulting list of adequate jurisdictions nonetheless coincides precisely with those that the European Commission had recognized as adequate at the time of adoption. See MARIANO PERUZZOTTI, PASADO, PRESENTE Y FUTURO DE LA TRANSFERENCIA INTERNACIONAL DE DATOS 40 (2d ed. 2021).

135. The list of countries recognized as providing adequate protection for personal data transfers from the European Union is maintained and updated by the European Commission. See *Adequacy Decisions*, EUR. COMM’N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/M358-F97V].

However, in Uruguay, this strategy introduces a structural vulnerability. Because such recognition mechanisms are tied to the validity of the EU–US framework, they become exposed to the same legal uncertainty that has repeatedly affected transatlantic data transfer arrangements.¹³⁶ The successive invalidations—first of the Safe Harbor and later of the Privacy Shield—illustrate the fragility of relying exclusively on the EU’s adequacy architecture. In this sense, third countries’ reliance on EU adequacy determinations effectively imports into their own legal systems the same instability that characterizes the transatlantic regulatory relationship.

Paradoxically, the emergence of unilateral recognition mechanisms by the United States as the ones described in Section III.B of this Article may mitigate this problem. If Latin American jurisdictions recognize the United States directly and independently—rather than adhering solely through frameworks negotiated with the European Union—the legal consequences of a future invalidation of an EU–US arrangement would be significantly reduced. In other words, the existence of a direct and autonomous recognition of the United States would decouple international data transfer regimes from the recurring judicial challenges affecting EU–US agreements, thereby alleviating what might otherwise become a recurring “Pandora’s box” problem in the global regulation of data flows.

A natural next question is whether the United States could extend the architecture of the EU–US Data Privacy Framework to Latin American partners. Following the Court of Justice of the European Union’s¹³⁷ decision in *Schrems II*, which invalidated the EU–US Privacy Shield adequacy decision, the United States was compelled to renegotiate the legal framework governing transatlantic data transfers with the European Union. This process ultimately resulted in the adoption of the EU–US Data Privacy

136. The Safe Harbor Agreement and the Privacy Shield framework constitute the two successive transatlantic data transfer mechanisms invalidated by the Court of Justice of the European Union in *Schrems I* and *Schrems II*, respectively. See Case C-362/14, *Schrems v. Data Prot. Comm’r (Schrems I)*, ECLI:EU:C:2015:650 (Oct. 6, 2015) (invalidating the Safe Harbor Agreement as incompatible with the fundamental right to privacy under EU law); Case C-311/18, *Data Prot. Comm’r v. Facebook Ir. Ltd.*, ECLI:EU:C:2020:559 (July 16, 2020) (invalidating the Privacy Shield framework and imposing heightened obligations on data exporters with respect to government access in recipient third countries).

137. See *Schrems II*, Case C-311/18, ECLI:EU:C:2020:559.

Framework,¹³⁸ which was supported by additional safeguards, including the creation of the Data Protection Review Court.¹³⁹

Subsequently, the United States extended the architecture of this framework to other jurisdictions, notably Switzerland¹⁴⁰ and the United Kingdom.¹⁴¹ In essence, these extensions reproduce, with necessary adaptations, the commitments and safeguards negotiated with the European Union and apply them in bilateral arrangements with third countries. From a regulatory perspective, this strategy allows the United States to build bridges with key trading partners in order to facilitate cross-border data transfers while leveraging the institutional and legal guarantees already negotiated with the European Union.

However, the United States has not demonstrated a willingness to extend the architecture of the Data Privacy Framework beyond a limited set of partners. In particular, it has not replicated a Data Privacy Framework-type arrangement for countries in Latin America; instead, cross-border transfers have been addressed through trade-based instruments and unilateral “adequacy”-style clauses.¹⁴²

138. See Commission Implementing Decision (EU) 2023/1795, *supra* note 126.

139. Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 14, 2022) (establishing the Data Protection Review Court as an independent adjudicatory body within the US Department of Justice to provide binding review of complaints submitted by individuals in qualifying states regarding the collection of their personal data through US signals intelligence activities); see also 28 C.F.R. pt. 201 (Attorney General regulations implementing the Data Protection Review Court pursuant to Executive Order 14,086).

140. See U.S. Dep’t of Commerce, *Swiss–U.S. Data Privacy Framework*, <https://www.dataprivacyframework.gov/s/participant-search/swiss-extension> [<https://perma.cc/WVC3-NPJJ>].

141. See U.S. Dep’t of Commerce, *U.K.–U.S. Data Bridge*, <https://www.dataprivacyframework.gov/s/participant-search/uk-extension> [<https://perma.cc/S3YG-NB9E>].

142. While the EU–US Data Privacy Framework is exclusively bilateral in scope, two additional jurisdictions have negotiated analogous arrangements modeled on its structure. The United Kingdom adopted the UK Extension to the EU–US Data Privacy Framework—formally denominated the Data Protection (Adequacy) (United States of America) Regulations 2023—which entered into force on October 12, 2023, enabling transfers of personal data from the United Kingdom and Gibraltar to US organizations certified under the Framework. Switzerland separately concluded the Swiss–US Data Privacy Framework, which became effective on September 15, 2024, upon recognition of adequacy by the Swiss Federal Council. See Data Protection (Adequacy) (United States of America) Regulations 2023, SI 2023/1028 (UK); Swiss Federal Council, Recognition of Adequacy for the Swiss–US Data Privacy Framework (Aug. 14, 2024); U.S. Dep’t of Commerce, *Data Privacy Framework Program*, <https://www.dataprivacyframework.gov> [<https://perma.cc/R68Q-SJMT>].

Although Argentina has pursued closer digital-trade alignment with the United States—framed publicly as a commitment to recognize the United States as an “adequate jurisdiction” for cross-border transfers of data, including personal data—the United States did not pursue an extension of the DPF architecture to cover Argentine data subjects. This is not a merely technical choice: The DPF’s legitimacy rests heavily on an independent, binding redress mechanism for complaints about US access to personal data, designed specifically for EU/European Economic Area (“EEA”) individuals and operationalized through a “qualifying state” channel for submitting complaints.

By declining to couple Latin American “trusted data” commitments with a comparable rights-and-remedies package, US practice effectively produces a two-tier model of digital trade: A fully institutionalized redress for European citizens, and lighter, trade-centered assurances for Latin American citizens.¹⁴³

D. The Promotion of the Cross-Border Privacy Rules System

Beyond unilateral adequacy recognitions, several of the United States’ Agreements on Reciprocal Trade with Latin American countries entrench the Washington Effect through a second, more operational mechanism: The express endorsement of the APEC Cross-Border Privacy Rules¹⁴⁴ (“CBPR”) system as a recognized framework for international personal data transfers. The CBPRs were originally developed within the Asia-Pacific Economic Cooperation (“APEC”) countries and relaunched globally through the Global CBPR Forum in June 2025. The CBPRs did not originate as a rights-based regulatory instrument, but as a trade-facilitation tool designed to reduce friction in cross-border digital commerce while preserving a minimal, interoperable baseline of privacy protection.

The CBPR system operates through an accountability-based, opt-in certification model.¹⁴⁵ Participating organizations

143. See PALAZZI, *supra* note 81, at 196 (stating that by withholding the extension of the Data Privacy Framework to Argentine citizens, the United States effectively subjects them to a lower standard of protection than that accorded to European citizens).

144. See GLOB. CROSS-BORDER PRIV. RULES F., <https://www.cbprs.org> [<https://perma.cc/QM73-ZSKY>].

145. Asia-Pacific Economic Cooperation [APEC], *Cross-Border Privacy Rules System Policies, Rules and Guidelines* (2019), <https://www.apec.org/docs/default-source/>

voluntarily commit to comply with common privacy standards, which are assessed and enforced by accredited accountability agents under domestic law.¹⁴⁶ Unlike the GDPR, CBPRs do not harmonize national legislation, displace domestic rules, or impose mandatory obligations across the board. Where domestic privacy law is weak or nonexistent, the CBPR framework supplies only a floor—not a ceiling—of protection. This structural flexibility makes CBPRs especially attractive as a complement to unilateral adequacy recognitions: Whereas adequacy decisions are jurisdiction-wide and politically visible, CBPR certification works at the organizational level, quietly operationalizing free data flows without reopening foundational legislative debates.

In this way, CBPRs actively contribute to the Washington Effect. By promoting a globally scalable, certification-based alternative to EU-style adequacy, trade agreements normalize a US regulatory logic in which data protection is framed as an enabler of commerce rather than as a constitutional right. The cumulative effect is not deregulation by rollback, but deregulation by bypass: Regulatory pressure shifts away from comprehensive rights-based reform, toward lighter, operational instruments that preserve access to US data markets while avoiding EU-level substantive commitments. CBPRs thus reinforce unilateral US adequacy recognitions by supplying the technical infrastructure through which those recognitions become economically meaningful.

The interface with the European Union exposes the sharp normative divergence between the two systems. Although both the GDPR and the APEC Privacy Framework trace their origins to Organisation for Economic Co-operation and Development (“OECD”) privacy principles, they have evolved along distinct constitutional paths. EU data protection law treats privacy as a fundamental right anchored in the Charter, whereas the CBPR treats it as a mechanism for trust and accountability in cross-border trade.¹⁴⁷ The CBPR system lacks core GDPR safeguards—

Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf [https://perma.cc/4S9M-9S9E] (establishing a voluntary, accountability-based certification mechanism through which organizations may demonstrate compliance with the APEC Privacy Framework as a condition for recognized cross-border data transfers among participating economies).

146. See Graham Greenleaf, *Five Years of the APEC Privacy Framework: Failure or Promise?*, 25 *COMPUT. L. & SEC. REP.* 28 (2009).

147. Yakovleva & Irion, *supra* note 122, at S80–82 (observing that the APEC accountability-based approach to transborder data transfers reflects an economic

such as rules on special category data, automated decision-making, children's data, data protection impact assessments, supervisory breach notification, and mandatory enforcement. For this reason, the CBPR framework is neither recognized as adequate nor capable of serving as a GDPR transfer mechanism.¹⁴⁸

Limited interoperability work was pursued between 2013 and 2014, when APEC and the EU's Article 29 Working Party mapped the substantive requirements of EU Binding Corporate Rules and the CBPR, developing a common referential to identify overlaps and gaps, and explored interoperability tools;¹⁴⁹ that work was placed on hold following the advent of the GDPR.¹⁵⁰ Although Article 42 of the GDPR¹⁵¹ leaves open the theoretical possibility of certification-based convergence, CBPRs remain, at present, normatively and legally external to the Brussels Effect.

For Latin American jurisdictions, CBPRs nonetheless offer a politically viable middle ground. The system is not new to the region: It has been explicitly contemplated in frameworks such as the USMCA, operationalized in Mexico for a short term,¹⁵² and has been shown to coexist with EU alignment in jurisdictions such as Japan. The European Commission has been unambiguous on this

paradigm that treats privacy as a mechanism for building commercial trust, in fundamental tension with the EU approach that treats data protection as a non-tradeable fundamental right anchored in the Charter of Fundamental Rights).

148. See Graham Greenleaf, *Global CBPRs: A Recipe for Failure?*, 177 PRIV. L. & BUS. INT'L REP. 11 (2022).

149. Article 29 Data Protection Working Party, *Opinion 02/2014 on a Referential for Requirements for Binding Corporate Rules Submitted to National Data Protection Authorities in the EU and Cross-Border Privacy Rules Submitted to APEC CBPR Accountability Agents*, 538/14/EN WP 212 (Feb. 27, 2014) [hereinafter *WP29 BCR/CBPR Referential*].

150. See CTR. FOR INFO. POL'Y LEADERSHIP, *CROSS-BORDER PRIVACY RULES, PRIVACY RECOGNITION FOR PROCESSORS, AND GDPR CERTIFICATIONS: FREQUENTLY ASKED QUESTIONS 7* (2023), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_prp_faqs_updated_july23.pdf [<https://perma.cc/LKP5-Q8AC>] ("Together they developed a common [referential]... [h]owever, this work was placed on hold due to other developments [significantly, the advent of the GDPR].").

151. GDPR, *supra* note 12, art. 42 (establishing a certification mechanism whereby controllers and processors may demonstrate compliance with the GDPR through approved certification bodies, seals, and marks).

152. In fact, Mexico had previously endorsed and operationalized the CBPR system: The former Mexican data protection authority, the INAI, established a dedicated CBPR office and actively participated in APEC fora, including its Data Privacy Subgroup. This institutional engagement constitutes a relevant precedent of the coexistence of CBPRs within a Latin American legal system.

point. In the EU's adequacy decision for Japan,¹⁵³ the European Commission stated that the APEC CBPR system offers protections "clearly of a lower level"¹⁵⁴ than those guaranteed by the GDPR, meaning that CBPR certification cannot be used for onward transfers of personal data originally transferred from the EU to Japan under the GDPR.

IV. THE TRADE AND/OR PRIVACY DEBATE: GEOPOLITICAL TENSIONS AND THE FUTURE OF CROSS-BORDER DATA RULES IN LATIN AMERICA

A. The "Washington Effect" as a Counter-Narrative to the Brussels Effect

Much scholarly attention has been devoted to the so-called "Brussels Effect." The "Brussels Effect" refers to the EU's capacity to export its regulatory standards to third countries through market power rather than formal legal obligation.¹⁵⁵ In the data protection context, the GDPR has driven third countries—including across Latin America—to enact comprehensive privacy legislation and establish independent supervisory authorities. Alignment with EU standards has effectively become a commercial prerequisite for continued access to the European market.

Yet a parallel and potentially countervailing dynamic has emerged in the region, one that may be provisionally termed the "Washington Effect." This phenomenon may be defined as the normative influence exercised by the United States over other

153. *EU-Japan Adequacy Decision*, *supra* note 123.

154. Recital 79 of the adequacy decision clarifies that, unless a third country has been formally recognized by the PPC as providing an equivalent level of protection, Japan restricts international transfers to mechanisms that create a legally binding relationship between the data exporter and the data importer and ensure adequate safeguards. As a result, non-binding frameworks—such as the APEC Cross-Border Privacy Rules (CBPR) system—are excluded, since they do not establish enforceable obligations between the parties and offer a lower level of protection than that required under the APPI and its Supplementary Rules.

155. BRADFORD, *supra* note 6, at 1–5 (defining the Brussels Effect as the EU's unilateral capacity to regulate global markets through the extraterritorial reach of its domestic standards, with data protection—and the GDPR in particular—constituting its most prominent contemporary manifestation); *see also* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012) (original law review article advancing the Brussels Effect thesis).

jurisdictions, including Latin America, through trade and investment agreements.

The operative effect of such instruments is to institutionalize the principle of free cross-border data flows toward the United States and its commercial operators, effectively displacing transfer restrictions, adequacy recognition requirements, and other sovereign regulatory tools that might otherwise restrict such transfers.

The Washington Effect, however, carries a structural paradox that demands critical scrutiny. The Brussels Effect drives third countries toward increasingly robust privacy standards modeled on the EU's rights-based framework and enforced through the adequacy mechanism. The Washington Effect operates in the opposite direction, promoting the liberalization of cross-border data flows and resisting regulatory constraints that might impede the free movement of personal data across borders. In the data protection context, the Washington Effect manifests not through the imposition of substantive privacy standards, but through the negotiation of bilateral and multilateral instruments designed to facilitate data transfers to jurisdictions that would not otherwise satisfy the EU's adequacy threshold. The two effects thus pull in structurally opposed directions: one conditions market access on regulatory convergence upward; the other seeks to preserve data flows regardless of the level of protection available at the destination. However, as of the time of this writing, the United States lacks a comprehensive federal data protection statute, does not possess an independent federal data protection supervisory authority with general enforcement jurisdiction, and does not recognize universal rights of access, rectification, or erasure comparable to those enshrined in Articles 15 through 17 of the GDPR.

The implications of this asymmetry are considerable from a conflicts-of-laws perspective. In the absence of Standard Contractual Clauses or equivalent transfer mechanisms providing a contractual choice-of-law or minimum substantive floor, data transferred to the United States will in all probability be governed by the law of the receiving jurisdiction, that is, the fragmented patchwork of sectoral federal statutes and state-level privacy laws that constitutes US data privacy law.

In a cross-border personal data transfer to a non-adequate jurisdiction like the United States, it would be self-defeating to treat the importer's domestic law (i.e., the law of the destination country) as the governing data-protection law, precisely because the transfer restrictions are triggered by the premise that the destination does not provide adequate protection.¹⁵⁶ In the realm of standard contractual clauses for international data transfers, the governing law for data-protection obligations in the transfer itself must always be the exporter's law—the law of the country of origin—otherwise, the entire protective logic of model clauses collapses. Accordingly, Latin American data subjects' personal data that migrates northward under the facilitative architecture of these trade agreements may become subject to an external legal regime affording substantially diminished normative protection relative to the exporting country's domestic framework.

In contrast to the prolonged and resource-intensive dialogue process that preceded the consolidation of the European data protection model, the United States managed to project regulatory influence within a matter of months rather than years.¹⁵⁷

Yet this influence did not operate through direct legal transplantation. The so-called Washington Effect is better understood as an indirect phenomenon: An exercise of structural power over data-related human rights through trade, market access, and geopolitical leverage—rather than through comprehensive statutory harmonization. US influence in the

156. See Yakovleva & Irion, *supra* note 122, at S83–85 (observing that the internal logic of the GDPR's transfer restriction regime presupposes the inadequacy of the destination country's domestic law as its very trigger, making reliance on that law as the governing standard structurally incompatible with the regime's purpose).

157. The contrast in pace and process is striking. Over the course of more than twenty-five years, the European Union recognized only three Latin American jurisdictions as providing adequate protection for personal data—Argentina, Uruguay, and Brazil—each following protracted bilateral dialogues, legislative reforms, and rigorous regulatory reviews. The United States, by contrast, negotiated Agreements on Reciprocal Trade with four Latin American countries—Argentina, Ecuador, El Salvador, and Guatemala—within a matter of months in 2025 and 2026, embedding data flow and digital trade provisions through commercial instruments that required no demonstration of substantive regulatory equivalence as a precondition. This divergence in tempo and methodology reflects a deeper structural difference between the two models: while the EU conditions the free movement of personal data on demonstrated convergence with its rights-based framework, the United States projects regulatory influence through trade agreements that prioritize market access and the liberalization of cross-border data flows over substantive privacy alignment.

privacy domain is thus best described as trade and privacy—but the US way: Sectoral enforcement, extraterritorial effects of commercial regulation, and contractual standard-setting, rather than a general federal privacy law.¹⁵⁸ The absence of federal laws is decisive. There are no unified guidelines capable of serving as a regulatory template for third countries, nor is it feasible to derive a coherent model from a patchwork of more than twenty state privacy statutes. As a result, convergence around the US approach has been limited and selective, reflecting dynamics of power and market dependence rather than a genuine process of normative diffusion.

B. The Dilution of “Adequacy” as a Normative Concept

If trade agreements continue to advance across Latin America along the model promoted by the United States (including a unilateral recognition of adequacy), the very meaning of adequacy as a normative concept risks being steadily diluted.

As more jurisdictions are required—through trade commitments rather than data protection reform—to recognize the United States as providing an “adequate” level of protection, adequacy will cease to function as the outcome of a substantive, two-level analysis grounded in law, institutions, and enforcement, and will instead become a by-product of market access negotiations. This dynamic is particularly destabilizing because adequacy has historically operated as a proxy for European Union standards, both within and beyond the EU legal order.

To date, none of the Latin American countries have recognized the United States as adequate via the data protection systems, except for Colombia in 2017, probably motivated by the historical commercial and political ties between the two countries.¹⁵⁹

158. See Schwartz & Peifer, *supra* note 102, at 128 (“Unlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action. There is also no requirement for the creation of statutory laws.”).

159. See *Colombia Designates U.S. as “Adequate” Data Transfer Nation*, HUNTON ANDREWS KURTH (Aug. 15, 2017), <https://www.hunton.com/privacy-and-cybersecurity-law-blog/colombia-designates-u-s-adequate-data-transfer-nation> [https://perma.cc/MXK8-6JLH].

Contrary to the United States' trade-centered strategy for "trusted data" arrangements, the European Union has limited its own room for maneuver: The EU has repeatedly maintained that personal data protection is not a negotiable trade term and must be insulated from trade bargaining.¹⁶⁰ This self-imposed separation reduces the European Union's capacity to deploy trade agreements as a vehicle for externalizing its preferred data-governance model.¹⁶¹ For example, the European Data Protection Supervisor ("EDPS") stated in February 2021 that personal data protection should not be subject to negotiation in the context of international trade agreements. In particular, the EDPS emphasized that digital trade agreements must preserve the high level of data protection guaranteed under EU law and the Charter of Fundamental Rights of the European Union, and warned that provisions on cross-border data flows should not undermine these safeguards. The EDPS therefore urged the European Commission to reaffirm the principle that privacy and data protection are fundamental rights rather than negotiable elements of trade policy.¹⁶²

The US approach represents the inverse strategy: Leveraging trade law to obtain the functional equivalent of adequacy without accepting its substantive constraints. This absence of substantive analysis is far from a trivial omission. As analyzed in Section III.A of this Article, the United States lacks a comprehensive federal privacy statute, does not regulate international data transfers accordingly, and offers no horizontally binding set of data-

160. Svetlana Yakovleva & Kristina Irion, *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, 10 INT'L DATA PRIVACY L. 201, 203-05 (2020) ("Data protection should not be subject to trade negotiations. It is a fundamental right, not a trade barrier, and as such, it should be fully excluded from these agreements.").

161. See Svetlana Yakovleva, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, 114 AJIL UNBOUND 10, 11-13 (2020) (arguing that the EU's negotiating position enshrines data protection as a fundamental right and creates a broad carve-out from trade liberalization commitments, thereby constraining the EU's capacity to use trade agreements as instruments for externalizing its preferred data governance model).

162. See *Data Protection Is Non-Negotiable in International Trade Agreements*, EUR. DATA PROT. SUPERVISOR (Feb. 22, 2021), https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en [<https://perma.cc/GA9T-HPV9>].

protection principles comparable in scope or enforceability to those embodied in the GDPR.

Equally problematic is the institutional dimension. To be sure, the redress architecture announced as the Privacy Shield successor was designed—through an executive order and implementing regulation—to address the independence and remedial authority concerns that EU institutions had raised in the Schrems saga and the ensuing negotiations. Yet, the durability of this design turns not only on formal institutional craftsmanship, but also on whether the resulting body can credibly satisfy EU law expectations of independence and effective remedy in practice—precisely the issues foregrounded by Professors Christakis, Propp, and Swire in their analysis of “essential equivalence”¹⁶³ and the final design of an independent redress authority with binding powers.¹⁶⁴

Recent events have exposed the fragility of US independent oversight bodies that are central to any credible adequacy assessment. The removal of a Federal Trade Commission Commissioner without statutory cause,¹⁶⁵ and the mass dismissal of Democratic members of the Privacy and Civil Liberties Oversight Board,¹⁶⁶ underscore the vulnerability of key privacy-relevant

163. See Théodore Christakis et al., *EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute Is Necessary to Produce an Essentially Equivalent Solution*, EUR. L. BLOG (Jan. 31, 2022), <https://www.europeanlawblog.eu/pub/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution> [https://perma.cc/3NMR-F7VT]; see also Théodore Christakis et al., *EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers*, EUR. L. BLOG (Feb. 16, 2022), <https://www.europeanlawblog.eu/pub/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers> [https://perma.cc/3NMR-F7VT].

164. See Théodore Christakis et al., *The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC*, IAPP (Oct. 11, 2022), <https://prod.iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/> (“As a general matter, what the new U.S. regime announced this week is consistent with the approach suggested in the articles. In both articles, we identified the redress-related deficiencies of Privacy Shield stated by the CJEU and other relevant EU legal institutions, and then discussed what possibilities existed under U.S. law to meet those legal requirements.”).

165. See *Trump v. Slaughter*, 146 S. Ct. 2883 (2026) (challenging statutory protections for the independence of Federal Trade Commission commissioners).

166. See Ella Lee, *Judge Finds Trump's Firing of Democrats on Privacy Oversight Board Unlawful*, HILL (May 21, 2025), <https://thehill.com/regulation/court-battles/5311867-judge-trumps-firing-democrats-privacy-oversight-board-unlawful> [https://perma.cc/5HUR-78WF].

institutions to political interference. These episodes are not peripheral to adequacy; they relate directly to the question of whether the United States can credibly guarantee independent supervision and effective enforcement of privacy—core elements of the “essentially equivalent” standard that adequacy is meant to embody and that the European Union is following closely.¹⁶⁷

Read through the lens of *Schrems II*, this trajectory is particularly troubling. In that case, the Court of Justice of the European Union made clear that adequacy hinges not on formal assurances or political commitments, but on the existence of durable, enforceable safeguards—especially independent oversight capable of constraining state surveillance.¹⁶⁸ The EU-US Data Privacy Framework itself rests in significant part on the institutional credibility of the Privacy and Civil Liberties Oversight Board as an external check on US intelligence practices.

Allowing the United States to obtain adequacy-like recognition through trade agreements, while the independence of precisely those institutions is openly contested, risks replicating the very deficiencies that *Schrems II* condemned. Adequacy thus becomes untethered from its constitutional function: Instead of signaling “essential equivalence,” it is reduced to a transferable label, insulated from judicial scrutiny and detached from the institutional guarantees on which transatlantic data flows are supposed to rest.

The tension between trade-based data governance and the data protection requirements emerging across Latin America is particularly acute in the context of adequacy and equivalence

167. See *Thought for the Week: Reflections on My IAPP Fireside Chat with Max Schrems*, IAPP (Apr. 6, 2026), <https://iapp.org/news/a/thought-for-the-week-reflections-on-my-iapp-fireside-chat-with-max-schrems> [<https://perma.cc/VP9H-GHSJ>] (“Schrems is still concerned about U.S. independence and enforcement for European privacy. He remains concerned with issues related to the independence of the U.S. Federal Trade Commission and the Privacy and Civil Liberties Oversight Board, and whether the U.S. system for substantive and procedural protections outlined in the DPF are working.”).

168. Case C-311/18, *Data Prot. Comm’r v. Facebook Ir. Ltd.* (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 105, 164–65, 179–85 (July 16, 2020) (holding that adequacy hinges not on formal political assurances but on the existence of durable, enforceable safeguards in the domestic legal order of the destination country, and finding the Privacy Shield invalid precisely because US surveillance programs were not limited to what was strictly necessary, did not grant data subjects actionable rights before independent courts, and the Ombudsperson mechanism failed to constitute a body sufficiently independent of the executive capable of imposing binding decisions on US intelligence services).

determinations. Several Latin American jurisdictions are actively pursuing or reconsidering their data protection frameworks with one eye on the requirements for obtaining adequacy recognition from the European Commission—a designation that would facilitate data transfers to and from the EU without additional safeguards.¹⁶⁹ The pursuit of European adequacy, however, may pull these jurisdictions toward regulatory models that are structurally incompatible with the commitments they have undertaken or may undertake in the context of trade agreements with the United States.

The inherent difficulty with the US position, however, lies in a structural contradiction that significantly limits its capacity to export a coherent regulatory model: The United States does not, in any meaningful sense, advocate for a competing data protection framework so much as it advocates for the absence of one.

The US posture in international data governance negotiations has been defined less by the promotion of specific substantive rights or enforceable obligations than by a consistent effort to preserve the conditions under which data flows freely across borders with minimal regulatory friction.¹⁷⁰ This is not a regulatory model in the conventional sense—it is, rather, a preference for deregulation dressed in the language of trade liberalization. And therein lies its fundamental limitation as an instrument of influence in Latin America: It is considerably easier to persuade a legislature to adopt rights than to persuade it to abandon them.

The political economy of data protection reform in Latin America reinforces this asymmetry. Across the region, data protection frameworks have been enacted—and in several jurisdictions are actively being strengthened—against a backdrop

169. Several Latin American jurisdictions are currently engaged in informal dialogues with the European Commission regarding potential adequacy determinations under the GDPR. These processes, however, are diplomatic in nature and do not follow a formally codified procedure or publicly established timeline; they depend on political will on both sides, legislative reform in the candidate jurisdiction, and the Commission's own prioritization of its adequacy review agenda.

170. Chander & Schwartz, *supra* note 120, at 68–72 (documenting the United States' sustained effort across successive administrations to embed data flow liberalization commitments in bilateral and multilateral trade agreements, prioritizing the removal of regulatory friction over the promotion of substantive privacy rights as the organizing principle of its international data governance strategy).

of constitutional recognition of privacy as a fundamental right, growing public awareness of data-related harms, and the institutional momentum of newly established or consolidating supervisory authorities. In this environment, the prospect of regulatory regression—of derogating existing rights, weakening enforcement mechanisms, or rolling back protections already embedded in domestic legal orders—faces formidable political and legal obstacles.

No government in the region has seriously entertained such a course, nor would the institutional actors most invested in data protection—including supervisory authorities, civil society organizations, and the academic community—permit it to advance without significant resistance. The direction of travel, in short, is toward stronger rather than weaker data protection, and US trade pressure is unlikely to reverse that trajectory.

C. The Internal Implementation of Unilateral Recognition in Trade Agreements: Future Challenges Ahead?

The unilateral recognition is not the end of a problem, but the beginning of a long domestic and judicial road. Even where a Reciprocal Trade instrument frames a data-transfer “recognition” in adequacy-like terms, the commitment still must clear domestic approval procedures, including ratification by the legislature of each relevant Latin American jurisdiction.

Moreover, because transfer regimes in the region frequently operate through administrative determinations, regulatory lists, or implementing acts by the local DPA (*see* Sections II.B.4 and III.C above), the practical effect of a trade-based recognition may depend on subsequent domestic action by the competent data protection authority, rather than being self-executing upon signature.¹⁷¹ This is especially likely where the instrument’s text reads as a programmatic commitment to regulatory alignment rather than an immediately operative amendment to the domestic transfer framework.¹⁷² In other words, the wording of the

171. *US–Argentina Agreement*, *supra* note 107, Annex III, § 2, ¶ 1 (“Argentina shall provide certainty regarding the ability to move personal data out of its territory to the United States including by recognizing the United States as a country or jurisdiction that provides adequate data protection under Argentina’s law.”).

172. 1 NÉSTOR PEDRO SAGÜÉS, *DERECHO CONSTITUCIONAL* 388–95 (2017) (distinguishing between self-executing and non-self-executing treaty provisions in

unilateral recognition proposed in the trade agreements (“shall provide certainty regarding the ability to move personal data out of its territory to the United States”) does not have direct effect and requires internal implementation in a way that has yet to be determined.

But the legal stakes rise sharply once these commitments collide with Latin America’s human-rights constitutional order. In some Latin American countries, ordinary treaties have precedence over ordinary legislation,¹⁷³ and in some cases, human rights treaties are equivalent to constitutional amendments.¹⁷⁴ One can expect the logical argument that a later trade instrument indirectly reshapes domestic data-transfer law by operation of internal hierarchy. But that move runs into some countervailing dynamics.

First, human rights treaties (recognizing privacy and data protection) rank above ordinary legislation and above ordinary treaties, so they cannot be modified by a subsequent trade agreement. Second, the Inter-American Court of Human Rights (the region’s highest human rights court) has recently recognized a right to informational self-determination as an autonomous right

Argentine constitutional law, and explaining that programmatic clauses require domestic legislative or regulatory implementation before they can generate individually enforceable rights).

173. See Art. 75, inc. 22, Constitución Nacional [Const. Nac.] (Arg.); see also Constituição Federal [C.F.] [Constitution] art. 5, § 3º (Braz.) (as amended by Emenda Constitucional No. 45 de 8 de dezembro de 2004); Constitución de la República del Ecuador [CRE] arts. 424–26 (2008) (Ecuador) (establishing that international treaties rank immediately below the Constitution in the normative hierarchy).

174. See Art. 75, inc. 22, Constitución Nacional [Const. Nac.] (Arg.) (as amended by Reforma Constitucional de 1994, Law No. 24430, Jan. 10, 1995, B.O. (Arg.)) (providing that treaties and concordats have hierarchical superiority over ordinary laws; that eleven enumerated international human rights instruments—including the American Declaration, the Universal Declaration, the American Convention on Human Rights, and the International Covenants—have constitutional rank in the conditions of their force and are to be understood as complementary to the rights and guarantees recognized in the first part of the Constitution; and that additional human rights treaties may be granted constitutional rank by a two-thirds vote of all members of each chamber of Congress); see also Constituição Federal [C.F.] [Constitution] art. 5, § 2º–3º (Braz.) (as amended by Emenda Constitucional No. 45, Dec. 8, 2004) (providing that international human rights treaties approved by three-fifths supermajority in both chambers shall be equivalent to constitutional amendments; all other rights recognized in treaties are incorporated by the open-ended rights clause of § 2º); Constitución de la República del Ecuador [CRE] arts. 424–26 (2008) (Ecuador) (establishing that international treaties rank immediately below the Constitution in the normative hierarchy; and that international human rights treaties recognizing rights more favorable than those contained in the Constitution shall prevail over any other legal norm or act of public power, including the Constitution itself).

in the *C.A.J.A.R. v. Colombia* judgment,¹⁷⁵ strengthening the regional baseline for data protection-related guarantees and for the availability of effective legal remedies to protect personal data. The lack of redress in the unilateral recognition of the United States and the refusal to extend the redress available in the Data Privacy Framework to Latin American jurisdictions poses a problem. Third, Argentina, Uruguay, and Mexico have become members of the Council of Europe's Convention 108 ecosystem (including the modernized Convention 108+ for at least Argentina and Uruguay), which carries its own internal logic for cross-border transfers and cooperation.¹⁷⁶

As a result, any "adequacy-by-trade" commitment raises classic treaty-interpretation questions—including how any subsequent trade instrument should be interpreted and reconciled within an existing data protection law, the human-rights treaty framework, and how it should be read within an already-operational transfer architecture under Convention 108/108+.¹⁷⁷ This could be particularly troublesome given that the United States is not a party to Convention 108 and has shown no indication of seeking entry into that system.

All of this creates fertile ground for "*Schrems*-style" litigation in Latin America. Once a trade-based recognition begins to operate domestically—whether via legislative approval, administrative implementation by the local data protection authority, or both—it becomes vulnerable to strategic challenges by civil-society actors. To challenge the treaty, they can frame the issue not as trade facilitation (and the important and obvious benefits it brings to the country), but as a mismatch between (i) an increasingly rights-based regional baseline (now reinforced by the recognition in Latin America of an autonomous informational self-determination right) and (ii) a transfer pathway grounded in political recognition of

175. *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CAJAR) v. Colombia*, Preliminary Objections, Merits, Reparations, and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 506 (Oct. 18, 2023) (recognizing, for the first time, *autodeterminación informativa* as an autonomous right).

176. Convention 108+, *supra* note 31, arts. 14–15, 17 (establishing in Chapter IV, Articles 14–15, a framework for cross-border transfers of personal data conditioned on the existence of an adequate level of protection in the recipient jurisdiction, and providing in Article 17 for cooperation mechanisms among supervisory authorities across contracting parties).

177. *Convention 108+*, *supra* note 31.

adequacy rather than shared membership in a rights-and-remedies regime.

As one example, Colombia's domestic "adequacy" designation of the United States in 2017 has not gone unchallenged: It is currently under judicial review before the Consejo de Estado in an annulment proceeding that has been awaiting a decision.¹⁷⁸ When the announcement of the US–Argentina trade agreement and the purported US adequacy determination became public, an Argentine member of Congress formally requested explanations from the national data protection authority (AAIP) regarding the legal basis, implementation mechanisms, and anticipated impact of the arrangement on the data protection rights of Argentine citizens.¹⁷⁹

The constitutional tensions generated by the US–Argentina agreement were not long in surfacing. In early 2026, following Argentina's signature of the Agreement on Reciprocal Trade and Investment ("ARTI") with the United States on February 5, 2026, a private individual challenged several of its provisions before the Argentine federal courts, invoking both a declaratory action of unconstitutionality and, in the alternative, a preventive habeas data claim.

The plaintiff argued that the ARTI could facilitate the transfer of personal data to third countries and thereby jeopardize constitutionally protected data protection rights.

The federal judge dismissed both claims, finding that no justiciable case or controversy existed: The ARTI had not yet entered into force—a process that is completed upon deposit of the instrument of ratification—and therefore could not yet produce legal effects capable of causing concrete injury to the plaintiff.¹⁸⁰ The court further held that the plaintiff lacked standing, as the alleged harms were merely hypothetical, and added that admitting

178. While the complaint was filed in 2022, the case remains pending without further judicial proceedings to date.

179. Hon. Cámara de Diputados de la Nación [HCDN], *Proyecto de Resolución (Pedido de Informes a la Agencia de Acceso a la Información Pública sobre el acuerdo con los Estados Unidos y la declaración de adecuación)*, Expte. No. 2898-D-2025 (Arg.), <https://rest.hcdn.gob.ar/web/proyectos/289888/adjuntos/104440> [<https://perma.cc/KVM5-SEYS>].

180. Juzgado Federal No. 2 de Mendoza [Juzg. Fed. Mza.] [Federal Court No. 2 of Mendoza], 19/6/2026, "Romano, Marcelo Martín c/ Estado Nacional – Poder Ejecutivo Nacional s/ Acción Declarativa de Inconstitucionalidad," Expte. No. FMZ 16128/2026 (Arg.).

such a claim would constitute an undue judicial interference in the Executive Branch's exclusive competence to negotiate and ratify international treaties. The decision remains subject to appellate review.¹⁸¹

In short, "unilateral recognition" is not the instant resolution of a transfer problem; it is the start of a contest over hierarchy, implementation, and legitimacy that the local and regional courts will need to hear and decide.

D. A Proposal: The Need to Regulate the Collection of Personal Data Online

Nelson Remolina Angarita's account of *recolección internacional de datos personales* (international data collection) offers a distinctly Latin American response to the Washington Effect—grounded not in trade commitments or unilateral adequacy pronouncements, but in the recalibration of local data protection doctrine to confront post-Internet realities.

Writing as early as 2015, Remolina¹⁸² argued that international data collection constitutes an analytically distinct phenomenon from traditional international data transfers—one that, in practice, poses even broader risks to personal data protection yet remains largely invisible within existing regulatory frameworks.

Remolina's core insight is architectural rather than merely doctrinal: While twentieth-century data protection regimes—from the OECD Guidelines and Convention 108 to the EU Data Protection Directive and the APEC Privacy Framework—were designed to regulate transfers of data sent abroad by domestic controllers, the Internet has inverted that logic. In the contemporary digital environment, platforms based in other countries routinely collect personal data directly from individuals located abroad, without any transfer ever occurring and therefore without triggering transfer-based safeguards. This regulatory blind spot, Remolina

181. See *Acuerdo entre Argentina y Estados Unidos: Rechazo de Acción Declarativa de Inconstitucionalidad*, ALLENDE & BREA (July 22, 2026), <https://allende.com/privacidad-y-ciberseguridad/acuerdo-entre-argentina-y-estados-unidos-rechazo-de-accion-declarativa-de-inconstitucionalidad-07-22-2026/> [<https://perma.cc/2UTJ-ZZAR>].

182. See REMOLINA ANGARITA, *supra* note 66. The book received the Spanish Data Protection Agency (AEPD) Personal Data Protection Award, recognizing its contribution to the development of privacy scholarship in the Spanish-speaking world. See *id.*

argues, enables large-scale cross-border processing to evade both national oversight and international coordination, even as its real-world impact exceeds that of classical transfer scenarios.

For Latin American jurisdictions in particular, Remolina shows how this gap translates into structural vulnerability: Individuals are exposed to pervasive data collection by platforms based abroad—often in the United States—operating entirely beyond the practical reach of domestic authorities. Because this data collection is not an international transfer, it does not need an SCC to be validated.¹⁸³

This diagnosis speaks directly to the Washington Effect identified in Section IV.A of this Article. Trade agreements that entrench free data flows function to protect precisely these actors, while simultaneously constraining the regulatory space Latin American states might otherwise deploy to impose equivalent obligations through local law. Remolina's normative intervention—calling for the explicit recognition and regulation of international data collection as a distinct legal category—thus represents an effort to reclaim regulatory agency through domestic norms, rather than conceding data governance to trade-based ordering alone.

V. CONCLUSION

This Article has shown that the governance of international transfers of personal data in Latin America can no longer be understood solely through the lens of the Brussels Effect. While EU data protection law, and particularly the GDPR, played a foundational role in shaping early Latin American privacy regimes and transfer mechanisms, recent developments reveal an emerging and increasingly influential effect of unilateral adequacy recognition through US trade agreements.

183. LUCA BELL, ANA BRIAN NOUGRÈRES, JUAN IGNACIO MENDOZA, PABLO A. PALAZZI & NELSON REMOLINA ANGARITA, *TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS NA AMÉRICA LATINA* (2024) (distinguishing international data collection—whereby a controller established in one jurisdiction directly collects personal data from individuals located in another jurisdiction without any transfer between data controllers or processors—from international data transfers properly so called, and concluding that the former does not constitute a transfer within the meaning of applicable data protection frameworks and therefore does not require standard contractual clauses or equivalent safeguards to be validated).

Latin America's data protection landscape has been shaped largely by the influence of the European regulatory model. Many countries in the region have adopted comprehensive personal data protection statutes inspired by European legislation and established supervisory authorities modeled on their European counterparts. This regulatory convergence has been reinforced by the European Union's adequacy decisions recognizing certain Latin American jurisdictions as providing an essentially equivalent level of protection, thereby enabling the free flow of personal data between those countries and the European Union.

With the unilateral "adequacy-like" approach that the United States has begun to deploy across Latin America, the European Union has effectively encountered a doppelgänger of its own adequacy concept—one that mirrors its function but not its substance. As described in Section III.B, EU adequacy is a complex and highly calibrated legal determination, structured as a multi-stage assessment grounded in fundamental rights, institutional independence, and enforceable guarantees.

By contrast, the US version of adequacy is obtained almost exclusively through regional trade agreements, stripped of the normative depth and rights-based architecture that characterize the European model. Most notably, this approach does not even extend to Latin American data subjects the safeguards that the United States itself was compelled to grant to European citizens under the EU-US Data Privacy Framework, thereby exposing a model of functional equivalence without constitutional or rights-protective symmetry.