IAI PAPERS 24 | 25 - SEPTEMBER 2024

ISSN 2610-9603 | ISBN 978-88-9368-344-9

Istituto Affari Internazionali

Transatlantic Cooperation on Data Governance and Digital Infrastructures

by Francesca Maremonti

Ministry of Foreign Affairs
and International Cooperation

ABSTRACT

The trajectory of transatlantic cooperation on data governance has been hampered by divergent principles on data protection and privacy, and by incidents which eroded the trust between the two partners. A lack of alignment on data governance to regulate the flow of data can disrupt cooperation between the European Union and the United States on cutting-edge digital infrastructure, with severe economic and national security ramifications. The cases of cloud services and subsea ICT cables expose how the unresolved trust deficit still constitutes an obstacle to transatlantic cooperation on critical digital infrastructures. Several avenues for cooperation have emerged as suitable dimensions to restore trust at the transatlantic level and address the challenges of the digital landscape. Nonetheless, significant challenges remain.

keywords

European Union | USA | Digital policy | Infrastructures | Transatlantic relations

Transatlantic Cooperation on Data Governance and Digital Infrastructures

by Francesca Maremonti*

Overview

Digitalisation – the so-called fourth industrial revolution – is changing how wars are fought, services are provided, money is transferred, and business is conducted between different countries.[1] The digital infrastructure that enables these transformations has become a battleground for geopolitical competition, with powers striving to secure leadership in a vast range of technologies, from data centres and clouds to 5G and 6G.

Digital infrastructure relies on the flow of data, much of which is dictated by national legislation, with governments seeking to establish sovereignty over data through a range of regulatory policies. Competing digital powers striving for leadership hold vastly different models for data governance, leaving the global architecture severely underdeveloped. In order to work together on the digital infrastructure required to keep pace in today's world, countries therefore need to improve their cooperation on the highly sensitive matter of data governance.

The European Union and the United States exchange more data than any other bilateral partnership in the world. This flow of data forms the backbone of the transatlantic digital economy, enabling 7.1 trillion US dollars of the EU-US economic partnership, and serves to protect personal privacy, human rights and national security interests.[2] And yet, there are stark differences in their data governance

[1] Sharinee Jagtiani, "The Global Cloudscape: The Geopolitics of Data Governance and Digital Power Play", in *Georgetown Journal of International Affairs*, 10 August 2023, https://gjia.georgetown.edu/?p=10241.

[2] US Department of Commerce, *Data Privacy Framework Program Launches New Website Enabling U.S. Companies to Participate in Cross-Border Data Transfers*, 17 July 2023, https://www.commerce.

* Francesca Maremonti is Research Fellow with the Multilateralism and Global Governance Programme at the Istituto Affari Internazionali (IAI).

· Paper produced in the framework of the project "La cooperazione economica e tecnologica Ue-Usa di fronte alle nuove sfide geostrategiche e il ruolo dell'Italia", conducted by IAI with the support of the Italian Ministry of Foreign Affairs and International Cooperation, the Fondazione Compagnia di San Paolo and the US Embassy to Italy. Views and opinions expressed are those of the author only.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

models, which are rooted in different values. This divergence could easily disrupt EU-US data flows, posing challenges to cooperation on digital infrastructure and therefore EU-US economic and security relations.

This paper explores the obstacles inhibiting cooperation on the data governance that underpins cutting-edge digital infrastructure. It begins by exploring the trajectory of EU-US cooperation on data governance, showing how the trust deficit between the transatlantic partners hampers cooperation, before considering the need to restore this trust in order to work together on cloud technology and the infrastructure required to enable it.

1. The trajectory of transatlantic data governance

Over the past decades, the EU and the US have undertaken several attempts to bridge the gap between their systems and promote cooperation on data governance. However, divergences over principles and various incidents that have eroded mutual trust have left them with a long way to go before achieving greater cooperation.

1.1 Divergences on principles

Approaches to data governance differ greatly across the Atlantic according to the respective conceptualisations of individual rights and the level of government involvement in data regulation.

The EU's model for data governance places significant weight on individual rights and data privacy, which is inscribed in the EU's Charter of Fundamental Rights (Article 7 and 8).[3] The EU's comprehensive data protection framework is primarily governed by the General Data Protection Regulation (GDPR), which imposes stringent measures on data holders and processors.[4] These principles extend beyond borders and also apply to cross-country data flows.[5] In the political guidelines for the 2019–2024 Commission, President of the European Commission Ursula von der Leyen stressed the need to "balanc[e] the flow and wide use of data while preserving high privacy, security, safety and ethical standards".[6] Over the past decades, the EU has adopted a cautious approach towards free data flow, trying to

gov/node/5386.

[3] European Union, *Charter of Fundamental Rights of the European Union*, 7 December 2000, http://data.europa.eu/eli/treaty/char_2012/oj.

[4] European Commission website: *Data Protection in the EU*, https://commission.europa.eu/node/2305_en.

[5] The EU has adopted a conditional approach to governing data flows between EU and non-EU countries. This means that only when such countries meet the EU's data protection requirements are cross-border data flows allowed.

[6] Ursula von der Leyen, *Political Guidelines for the Next European Commission 2019-2024*, Luxembourg, Publications Office of the European Union, 2020, p. 13, https://doi.org/10.2775/101756.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

integrate its high data protection standards into bilateral trade agreements. The first one was sealed under the 2019 Economic Partnership Agreement (EPA) with Japan, which included a commitment from the two parties to introduce cross-border data flow clauses under the EPA, within three years of the agreement's entry into force.[7]

The United States' stance on data governance reflects a market-driven approach, which sees data as a trade commodity used by business actors.[8] Despite being on the Congressional to-do list for years,[9] the United States has yet to establish a comprehensive federal law for data protection.[10] The US "techno-positivist" approach – linking data-driven technical innovation to economic growth – has resulted in limited government interventions in data flow regulation.[11] Privacy and data protection regulations vary across industries and are enforced by different agencies, resulting in a diverse and fragmented privacy landscape.[12]

1.2 The transatlantic trust deficit

Despite divergences over the principles that regulate their data governance, in recent years the EU and the United States have doubled down on their efforts to increase convergence.

The EU and the United States began to regulate governance of transatlantic data flows with the adoption of the Safe Harbour agreement in 2000. Over the fifteen years during which Safe Harbour served as a framework for cross-country data flow, the EU became increasingly preoccupied with the adequacy of data privacy protection.[13] Importantly, the Safe Harbour framework did not address the normative differences on data governance between the partners.

[7] European Commission DG Trade website: *EU-Japan Economic Partnership Agreement*, https://policy.trade.ec.europa.eu/node/668_en.

[8] Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology*, Oxford, Oxford University Press, 2023.

[9] Several states have passed their own laws (California, Virginia, Colorado, Utah and Connecticut), setting a trend likely to be followed by many others.

[10] Hung Tran, "Competing Data Governance Models Threaten the Free Flow of Information and Hamper World Trade", in Atlantic Council Issue Briefs, November 2021, https://www.atlanticcouncil.org/?p=460660.

[11] Julia Pohle, *Digital Sovereignty. A New Key Concept of Digital Policy in Germany and Europe*, Berlin, Konrad-Adenauer-Stiftung, 2020, p. 7, https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet.

[12] Federica Marconi, "The EU–US Data Protection Framework: Balancing Economic, Security and Privacy Considerations", in *IAI Commentaries*, No. 23|46 (September 2023), https://www.iai.it/en/node/17505.

[13] Xinchuchu Gao and Xuechen Chen, "Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions", in *EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, 2024, p. 50-56, https://doi.org/10.1145/3655693.3655720.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

In 2013 this fragile institutional balance on data governance experienced a shock. The Edward Snowden whistleblowing case unveiled a mass surveillance scandal involving the US intelligence collecting, storing and analysing citizens' data.[14] This was found to be in violation of the EU's data protection laws and the fundamental rights of EU citizens.[15] Two years later, the data activist Max Schrems challenged the Safe Harbour framework before the Court of Justice of the European Union (CJEU) for breaching EU law under the EU-US data sharing arrangement.[16] In 2015 the court ruled that US public authorities had failed to provide adequate levels of protection for data privacy as required by EU law, invalidating the Safe Harbour agreement.[17]

The legal uncertainty and mistrust that followed was offset by the urgency to provide an EU-US data transfer agreement for the 4,500 businesses left without a legal framework for their activities.[18] In February 2016, the European Commission and the US' Department of Commerce jointly announced the adoption of the Privacy Shield principles to regulate transatlantic data governance.[19] In July 2020, in the second episode of what became known as the "Schrems saga", Schrems again challenged Privacy Shield before the CJEU. The court then invalidated the Privacy Shield principles, ruling that it did not offer the necessary level of protection to comply with EU standards for personal data transfer, by then enshrined in the 2016 GDPR.[20] These episodes cemented the EU's persistent concerns over the United States' lack of data protection, generating a trust deficit which breached transatlantic cooperation on data governance.

1.3 Towards greater cooperation

Following the CJEU's decision, the EU and United States again engaged in intensive negotiations. These efforts culminated in the adoption of the EU-US Data Privacy

[14] Sergio Carrera, *EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy. CEPS Task Force Outline*, 7 December 2023, https://www.ceps.eu/?p=41623.

[15] Ibid.

[16] Ibid.

[17] Shara Monteleone and Laura Puccio, "From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules", in *EPRS In-depth Analysis*, January 2017, https://doi.org/10.2861/09488.

[18] Joshua P. Meltzer, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, Testimony before the US House of Representatives Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology, Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows", 3 November 2015, https://www.brookings.edu/?p=81397.

[19] European Commission, *Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, http://data.europa.eu/eli/dec_impl/2016/1250/oj.

[20] Nigel Cory, Daniel Castro and Ellysse Dick, *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, Washington, Information Technology & Innovation Foundation, December 2020, https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

Framework of July 2023.[21] This new framework seeks to address the concerns raised in the Schrems II ruling by introducing measures such as limiting US surveillance activities to what is necessary and proportionate for national security and establishing a two-tier redress mechanism for individuals.

In recent years, noteworthy developments have also unfolded on the American side of the Atlantic, most notably the proposal for an American Data Privacy Protection Act (ADPPA).[22] Introduced in June 2022, this bipartisan bill aimed to create a comprehensive federal privacy framework, reflecting several principles similar to the EU's GDPR concerning data privacy. The ADPPA would have represented a significant shift in the United States' approach to data privacy, influenced by the EU's regulatory standards, often referred to as the "Brussels effect", but was never passed.[23] In April 2024, the American Privacy Rights Act (APRA) bill was then proposed on similar principles to the original ADPPA.[24] The draft of the APRA is currently at the introductory level and still needs to undergo bicameral voting, before being passed into law.[25] If approved, APRA would constitute the first comprehensive federal consumer privacy framework.[26]

In conclusion, there are still significant divergences between the EU and US legal frameworks and a degree of distrust between the parties. It is therefore necessary for the two partners to continue to work towards further alignment of data governance.

2. From data governance to digital infrastructures

A lack of alignment on data governance to regulate the flow of data can easily hamper cooperation between the EU and the United States on cutting-edge digital infrastructure, with severe economic and national security ramifications. In today's interconnected world, digital infrastructure often unfolds on a global scale, which is at odds with nationally determined regulations. The cloud is an illustrative example of this tension and the ensuing consequences.

[21] European Commission, *Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows*, 10 July 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

[22] Consumer Privacy Act website: *American Data Privacy and Protection Act (ADPPA)*, https://www.consumerprivacyact.com/?p=342.

[23] Xinchuchu Gao and Xuechen Chen, "Understanding the Evolution of Transatlantic Data Privacy Regimes", cit.

[24] Perla Khattar, "The American Privacy Rights Act of 2024 Explained: What Does the Proposed Legislation Say, and What Will it Do?", in *Tech Policy Press*, 9 April 2024, https://www.techpolicy.press/the-american-privacy-rights-act-of-2024-explained-what-does-the-proposed-legislation-say-and-what-will-it-do.

[25] US Congress, *H.R.8818 - American Privacy Rights Act of 2024*, 25 June 2024, https://www.congress.gov/bill/118th-congress/house-bill/8818.

[26] Chris D. Linebaugh et al., "The American Privacy Rights Act", in *CRS Legal Sidebar*, No. LSB11161 (updated 31 May 2024), https://crsreports.congress.gov/product/details?prodcode=LSB11161.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

2.1 The cloud

The cloud is a vast network of remote servers around the globe that operate as a single ecosystem. It provides the infrastructure to store and manage data needed to run applications and deliver content or services, like emails and social media.[27] Over the past decade, cloud technology has emerged as a crucial enabler for business digitalisation, the delivery of public services and conflict management.[28] More than 80 per cent of organisations globally are either using or planning to adopt cloud technology by 2025[29] and the cloud market is expected to grow in the coming years, reaching an estimated value of 2,321 billion US dollars by 2032.[30] The growing potential of the cloud has made this digital infrastructure a battleground for geopolitical competition between actors striving for leadership. For example, China and the United States are racing for their respective cloud service providers to move ahead of each other in the international cloud services market.[31] But given that cloud technology raises issues concerning digital sovereignty and data governance as well, EU and US regulators are faced once again with their unresolved trust deficit.

The cloud market is currently dominated by a handful of American cloud providers – called hyperscalers – such as Microsoft Azure, Amazon Web Services, Google Cloud and IBM Cloud.[32] These hyperscalers store and process the data of European governments – including critical data on health and defence. In 2018, the United States introduced the Cloud Act, which grants authorities the power to access data held on servers of American tech companies, regardless of whether the data is stored outside US borders.[33] The cloud as a transnational business, delivered by companies operating a globally distributed digital infrastructure, challenges the EU's drive to pursue digital sovereignty, as hyperscalers are subject to extra-territorial legislation.[34]

[27] Microsoft Azure website: *What Is the Cloud?*, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud.

[28] Sharinee Jagtiani, "The Global Cloudscape", cit.

[29] Max Peterson, "How AWS Can Help You Navigate the Complexity of Digital Sovereignty", in *AWS Security Blog*, 7 February 2024, https://aws.amazon.com/blogs/security/how-aws-can-help-you-navigate-the-complexity-of-digital-sovereignty.

[30] Market.Us, "Cloud Computing Market to Reach USD 2,321.1 Billion by 2032: Exploring the Diverse Applications of Cloud Computing", in *GlobeNewswire*, 17 March 2023, https://www.globenewswire.com/en/news-release/2023/03/17/2629610/0/en/Cloud-Computing-Market-to-Reach-USD-2-321-1-Billion-by-2032-Exploring-the-Diverse-Applications-of-Cloud-Computing.html.

[31] Leading Chinese Cloud providers: Tencent and Alibaba.

[32] Filippo Gualtiero Blancato and Madeline Carr, "The Trust Deficit. EU Bargaining for Access and Control over Cloud Infrastructures", in *SSRN*, 27 May 2024, https://ssrn.com/abstract=4843466.

[33] US Department of Justice Criminal Division, *CLOUD Act Resources*, updated on 14 October 2023, https://www.justice.gov/criminal/cloud-act-resources.

[34] Cloud service providers store data in multiple data centres, sometimes in different countries. Such data flows across servers to be accessed by users from any location. Furthermore, data is generally copied and held in various locations to avoid potential disruptions.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

American cloud providers have designed measures tailored to the EU's concerns over data sovereignty. For example, in 2023 Microsoft set up the EU Data Boundary to address issues concerning EU data localisation.[35] Under the EU Data Boundary, European commercial and public sector data are stored by the cloud provider within the borders of the EU.[36] Hyperscalers are seeking to bridge the trust deficit and comply with the EU's quest for sovereignty over its data providing technical solutions.

The trust issue which underpins data governance for the cloud cannot be bridged with technical solutions. Several European governments have started to turn to European-designed cloud solutions.[37] In 2019 the EU launched the Gaia-X project, an initiative to develop a federal cloud complying with European values and data protection regulation. Gaia-X was envisioned as an interconnected network of data centres and cloud services distributed across different member states. Despite the initial optimism, Gaia-X struggled to get off the ground and has not delivered a European data cloud to this day.[38]

Mistrust and diverging data governance approaches are likely to result in a lower uptake of cloud technology from the European side, potentially harming the region's economic growth.[39] While US cloud providers have offered ad-hoc solutions for the EU's concerns over data management in the cloud, US policymakers', with their "hands-off" approach towards technology regulation, have not provided policy responses and measures to comply with the EU's data protection standards for cloud services.

2.2 ICT cables

The physical infrastructure that enables the cloud illustrates the need for international cooperation between partners when it comes to data governance. Data flow to and from the cloud relies on cables, which run over land or under the sea. It is estimated that 99 per cent of internet traffic passes through fibre-optic submarine cables.[40]

[35] Microsoft website: *EU Data Boundary*, https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb.

[36] Ibid.

[37] Tambiama Madiega, "Digital Sovereignty for Europe", in *EPRS Briefings*, July 2020, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992.

[38] Clothilde Goujard and Laurens Cerulus, "Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project", in *Politico*, 26 October 2021, https://www.politico.eu/?p=1855905.

[39] Filippo Gualtiero Blancato and Madeline Carr, "The Trust Deficit", cit.; Matthias Bauer and Philipp Lamprecht, "The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States", in *ECIPE Occasional Papers*, No. 4/2023 (October 2023), https://ecipe.org/?p=89730.

[40] Julia Tréhu and Megan Roberts, "Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective", in *IAI Papers*, No. 24|04 (February 2024), https://www.iai.it/en/node/18148.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

As the world we live in gets increasingly digitised, countries have doubled down on their efforts to gain a share of the submarine ICT cable market. China, with its Digital Silk Road global project, has made connectivity a pillar of its international engagements. The Peace ICT cable is its flagship project in this regard. The EU has also scaled up investments to expand its footprint on global connectivity projects, including submarine cables, under the Global Gateway, the EU's strategy for global infrastructural and development investments launched in 2021. Subsea ICT cables feature prominently even within projects promoted by USAID, the US international development agency.

Today the major submarine cable companies are the US SubCom, the Japanese NEC Corporation, France's Alcatel Submarine Networks and Chinese HMN Tech.[41] In recent years, American "hyperscalers" – Google, Meta, Amazon and Microsoft – have substituted the traditionally state-backed companies responsible for the laying of the cables. US hyperscalers are now involved in nearly every cable laid as providers.[42]

ICT cables, laying at the bottom of the sea, are exposed to a range of deliberate or accidental damage. Over the years, incidents have spanned from fishing ships' anchors accidentally cutting the cables to malicious attacks aimed at severely disrupting the services of a targeted country or region or to tap into the cables and eavesdrop. These incidents expose a number of vulnerabilities involving the "naked infrastructure", the cable, as well as the "soft layer", the data flowing within.[43] Concerning the maintenance of the damaged cables, international law is still underdeveloped and there is a degree of unclarity on responsibility and accountability of actors when incidents occur in international waters.[44] Additionally, only a handful of countries own vessels designed for cable maintenance, due to the high costs. Chinese's Jiaolong and Russian Losharik are among these.[45] There are mounting concerns over maintenance companies' potential to tap into the cables and over data protection within ICT cables. Given the massive economic, political and security ramifications of ICT submarine cables, countries have acknowledged the need to cooperate and ensure resilient and secure networks of infrastructures.

The EU and the United States are cooperating on a number of ICT cable projects. The Sea-Me-We-6 submarine cable is currently the most important element of transatlantic cooperation in the provision of digital infrastructure and has the

[41] Ibid.

[42] Alan Mauldin, "A (Refreshed) List of Content Providers' Submarine Cable Holdings", in *TeleGeography Blog*, 27 June 2024, https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new.

[43] Anselm Küsters, André Wolf and Eleonora Poli, "Challenges to Transatlantic Digital Infrastructure: An EU Perspective", in *IAI Papers*, No. 24|03 (February 2024), https://www.iai.it/en/node/18132.

[44] Amy Paik and Jennifer Counter, "International Law Doesn't Adequately Protect Undersea Cables. That Must Change", in *Hybrid Conflict Project Commentaries*, 25 January 2024, https://www.atlanticcouncil.org/?p=727834.

[45] Ibid.

IAI PAPERS 24 | 25 - SEPTEMBER 2024
ISSN 2610-9603 | ISBN 978-88-9368-344-9

potential to provide an alternative to China's Peace cable. However, on the "soft layer" side of cooperation, Brussels has shown growing apprehension over the risk of surveillance of data by the companies involved in the laying and in the maintenance of cables, including American ones.[46] The EU's Cyber Resilience Act, approved in March 2024, requires the manufacturers of connectable hardware and software products to protect the confidentiality and integrity of data.[47] Moreover, in January 2024, under the EU's Digital Networks Act (DNA), the Commission introduced possible actions to foster the innovation, security and resilience of digital infrastructures, many addressing ICT cables.[48] These measures predominantly push for further coordination at the EU level, but they also encourage cooperation among stakeholders, member states and like-minded partners.[49] To build a stronger ecosystem for digital infrastructures, cooperation on the "naked infrastructure" is not sufficient. A comprehensive approach encompassing deepened alignment on the protection of the data flowing within the infrastructure could set the ground for stronger transatlantic cooperation.

3. Avenues for cooperation

In recent years, efforts to enhance cooperation on data governance have been scaled up at the bilateral, regional and international level. This is a positive premise for building a higher degree of normative convergence between the EU and the United States and strengthen cooperation on digital infrastructures. However, significant challenges remain.

In 2021, the US–EU Trade and Technology Council (TTC) was established as a new transatlantic platform to facilitate cooperation and coordinate action on issues ranging from technology standards and global trade to security of supply chains.[50] One of the ten thematic working groups of the TTC is dedicated to "data governance and technology platforms". Many observers have pointed out that the TTC, as a non-binding framework, has not addressed regulatory divergences and provided mixed results in tackling data policy issues.[51] But the TTC has emerged as an avenue to address challenges concerning emerging technologies and digital infrastructures. For example, one working group of the TTC is designed for "ICTS security and competitiveness". And while a tangible outcome on the matter has yet to

[46] Anselm Küsters, André Wolf and Eleonora Poli, "Challenges to Transatlantic Digital Infrastructure", cit.

[47] Cyber Risk GmbH, *The Digital Networks Act (DNA)*, https://www.digital-networks-act.com.

[48] Ibid.

[49] European Commission, *Commission Presents New Initiatives for Digital Infrastructures of Tomorrow*, 21 February 2024, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_941.

[50] US Department of State website: *U.S.-EU Trade and Technology Council (TTC)*, https://www.state.gov/u-s-eu-trade-and-technology-council-ttc.

[51] Frances Burwell and Andrea G. Rodríguez, "The US-EU Trade and Technology Council: Assessing the Record on Data and Technology Issues", in *Atlantic Council Issue Briefs*, April 2023, https://www.atlanticcouncil.org/?p=620980.

ISSN 2610-9603 | ISBN 978-88-9368-344-9

materialise, the working group has flagged its commitment to address transatlantic subsea cables' connectivity and security as a future priority.[52] The cloud does not feature as a priority among the TTC deliverables and transatlantic cooperation in this sector remains uncharted. The future of the TTC is evidently uncertain at a time of increased political volatility. A potential change of administration across the Atlantic could be a disrupting factor for the continuity of the TTC's outputs.

The trust deficit impairing transatlantic cooperation on data governance has thus not been fully restored. The EU and the United States should build on their respective cooperative ties with third actors and draw from existing models and best practices for data governance. For example, the commitment made in the aforementioned 2019 EU-Japan Economic Partnership Agreement was cemented in 2023, when the EU and Japan concluded an agreement on cross-border data flow.[53] This landmark agreement can serve as a model to integrate data regulation standards under bilateral trade agreements, a model which could be adopted by countries beyond the EU-Japan when designing future economic partnerships.

Multilateral fora can also be suitable avenues for sharing best practices among key actors trying to address the challenges of the digital landscape. The concept of Data Free Flow with Trust (DFFT) was introduced within the G20 framework in 2019, to promote the free flow of data while ensuring trust in privacy, security and intellectual property rights. The DEFT was further developed at the Japanese G7 summit in Hiroshima in 2023, with the establishment of the Institutional Arrangement for Partnership to operationalise it. The G20, bringing together different models of data governance, can serve as a platform to exchange best practices. India, for example, has promoted a model of data governance for its digital public infrastructure, aimed at boosting economic growth, which is worth considering. For the cloud, India has adopted a model which invites domestic and foreign companies to apply to be providers, which has resulted in the Indian cloud market outpacing the global average.[54] While the EU and the United States US double down on their effort to restore their trust deficit at the bilateral level, their partnership could be strengthened within broader cooperation frameworks, and benefit from the exchange of best practices with other key actors.

Policy recommendations

Reinvigorate and reshape the TTC. – While it is essential to preserve an avenue for transatlantic bilateral cooperation on data governance and digital infrastructures,

[52] Trade and Technology Council, *EU-US Joint Statement of the Trade and Technology Council*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516.

[53] European Commission, *EU and Japan Conclude Landmark Deal on Cross-Border Data Flows at High-Level Economic Dialogue*, 28 October 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378.

[54] Sharinee Jagtiani, "The Global Cloudscape", cit.

IAI PAPERS 24 | 25 - SEPTEMBER 2024 ISSN 2610-9603 | ISBN 978-88-9368-344-9

it is paramount that such an avenue addresses the main challenges involved in the partnership. Data governance remains a core challenge, partially unresolved at the TTC level. Data governance underpins transatlantic cooperation on a number of critical sectors, including digital infrastructures such as cloud services and ICT cables. The structure of the TTC should therefore integrate data governance as a cross-cutting theme, rather than narrowing the purpose of cooperation on data governance to one distinct working group.

Design a code of conduct for cloud developers. – Transatlantic cooperation on the cloud has a long way to go. Mistrust and concerns over sovereignty of data remain an obstacle to EU-US cooperation in the cloudscape. The EU and the United States should draw from existing practices of standard setting, such as the Code of Conduct for AI developers, released under Japan's G7 presidency in 2023. A code of conduct for cloud developers, setting standards for data protection in the cloud, should merge a normative effort with technical measures, bringing together the various stakeholders involved – from the private sector to policymakers – from both sides of the Atlantic. A code of conduct for cloud developers could be a building block to overcome the transatlantic trust deficit and increase cooperation in this sector.

Promote a multi-layer approach to subsea ICT cable cooperation. – The EU and the United States have flagged their commitment to enhance the resilience of submarine ICT cables and to expand their footprint on global connectivity projects. However, cooperation efforts have predominantly centred around the physical infrastructure, overlooking the "soft layer" involving data security. The EU and the United States should carve multi-stakeholder working groups within existing ICT cooperation platforms – whether within the TTC or beyond - to promote data governance for submarine ICT cables. Their efforts should address: risk assessment; monitor incidents to cable-laying and management and identify vulnerabilities for data security; establishing protocols for incident response to comply with existing data regulation frameworks; working towards international standard-setting.

Enhance transatlantic cooperation through broader fora. – The challenges involved in transatlantic cooperation in the field of data governance and digital infrastructures are not unique to this partnership. The global dimension of the digital economy, cyber security and digital infrastructures requires a global approach. While restoring the transatlantic trust deficit is crucial, the EU and the United States should draw from models advanced by third actors. The transatlantic partnership should leverage the strengths of each model of data governance, increasing the share of best practices among key actors pioneering the digital landscape.

Updated 10 September 2024

IAI PAPERS 24 | 25 - SEPTEMBER 2024 ISSN 2610-9603 | ISBN 978-88-9368-344-9

References

Matthias Bauer and Philipp Lamprecht, "The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States", in *ECIPE Occasional Papers*, No. 4/2023 (October 2023), https://ecipe.org/?p=89730

Filippo Gualtiero Blancato and Madeline Carr, "The Trust Deficit. EU Bargaining for Access and Control over Cloud Infrastructures", in *SSRN*, 27 May 2024, https://ssrn.com/abstract=4843466

Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology*, Oxford, Oxford University Press, 2023

Frances Burwell and Andrea G. Rodríguez, "The US-EU Trade and Technology Council: Assessing the Record on Data and Technology Issues", in *Atlantic Council Issue Briefs*, April 2023, https://www.atlanticcouncil.org/?p=620980

Sergio Carrera, *EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy. CEPS Task Force Outline*, 7 December 2023, https://www.ceps.eu/?p=41623

Nigel Cory, Daniel Castro and Ellysse Dick, *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, Washington, Information Technology & Innovation Foundation, December 2020, https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic

European Commission, *Commission Presents New Initiatives for Digital Infrastructures of Tomorrow*, 21 February 2024, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_941

European Commission, *Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows*, 10 July 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

European Commission, *EU and Japan Conclude Landmark Deal on Cross-Border Data Flows at High-Level Economic Dialogue*, 28 October 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378

European Commission, *Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, http://data.europa.eu/eli/dec_impl/2016/1250/oj

European Union, *Charter of Fundamental Rights of the European Union*, 7 December 2000, http://data.europa.eu/eli/treaty/char_2012/oj

ISSN 2610-9603 | ISBN 978-88-9368-344-9

Xinchuchu Gao and Xuechen Chen, "Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions", in *EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, 2024, p. 50-56, https://doi.org/10.1145/3655693.3655720

Clothilde Goujard and Laurens Cerulus, "Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project", in *Politico*, 26 October 2021, https://www.politico.eu/?p=1855905

Sharinee Jagtiani, "The Global Cloudscape: The Geopolitics of Data Governance and Digital Power Play", in *Georgetown Journal of International Affairs*, 10 August 2023, https://gjia.georgetown.edu/?p=10241

Perla Khattar, "The American Privacy Rights Act of 2024 Explained: What Does the Proposed Legislation Say, and What Will it Do?", in *Tech Policy Press*, 9 April 2024, https://www.techpolicy.press/the-american-privacy-rights-act-of-2024-explained-what-does-the-proposed-legislation-say-and-what-will-it-do

Anselm Küsters, André Wolf and Eleonora Poli, "Challenges to Transatlantic Digital Infrastructure: An EU Perspective", in *IAI Papers*, No. 24|03 (February 2024), https://www.iai.it/en/node/18132

Chris D. Linebaugh et al., "The American Privacy Rights Act", in *CRS Legal Sidebar*, No. LSB11161 (updated 31 May 2024), https://crsreports.congress.gov/product/details?prodcode=LSB11161

Tambiama Madiega, "Digital Sovereignty for Europe", in *EPRS Briefings*, July 2020, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992

Federica Marconi, "The EU–US Data Protection Framework: Balancing Economic, Security and Privacy Considerations", in *IAI Commentaries*, No. 23|46 (September 2023), https://www.iai.it/en/node/17505

Market.Us, "Cloud Computing Market to Reach USD 2,321.1 Billion by 2032: Exploring the Diverse Applications of Cloud Computing", in *GlobeNewswire*, 17 March 2023, https://www.globenewswire.com/en/news-release/2023/03/17/2629610/0/en/Cloud-Computing-Market-to-Reach-USD-2-321-1-Billion-by-2032-Exploring-the-Diverse-Applications-of-Cloud-Computing.html

Alan Mauldin, "A (Refreshed) List of Content Providers' Submarine Cable Holdings", in *TeleGeography Blog*, 27 June 2024, https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new

Joshua P. Meltzer, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, Testimony before the US House of Representatives Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology, Hearing on "Examining the EU Safe Harbor

ISSN 2610-9603 | ISBN 978-88-9368-344-9

Decision and Impacts for Transatlantic Data Flows", 3 November 2015, https://www.brookings.edu/?p=81397

Shara Monteleone and Laura Puccio, "From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules", in *EPRS In-depth Analysis*, January 2017, https://doi.org/10.2861/09488

Amy Paik and Jennifer Counter, "International Law Doesn't Adequately Protect Undersea Cables. That Must Change", in *Hybrid Conflict Project Commentaries*, 25 January 2024, https://www.atlanticcouncil.org/?p=727834

Max Peterson, "How AWS Can Help You Navigate the Complexity of Digital Sovereignty", in *AWS Security Blog*, 7 February 2024, https://aws.amazon.com/blogs/security/how-aws-can-help-you-navigate-the-complexity-of-digital-sovereignty

Julia Pohle, *Digital Sovereignty. A New Key Concept of Digital Policy in Germany and Europe*, Berlin, Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet

Trade and Technology Council, *EU-US Joint Statement of the Trade and Technology Council*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516

Hung Tran, "Competing Data Governance Models Threaten the Free Flow of Information and Hamper World Trade", in *Atlantic Council Issue Briefs*, November 2021, https://www.atlanticcouncil.org/?p=460660

Julia Tréhu and Megan Roberts, "Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective", in *IAI Papers*, No. 24|04 (February 2024), https://www.iai.it/en/node/18148

US Congress, *H.R.8818 - American Privacy Rights Act of 2024*, 25 June 2024, https://www.congress.gov/bill/118th-congress/house-bill/8818

US Department of Commerce, *Data Privacy Framework Program Launches New Website Enabling U.S. Companies to Participate in Cross-Border Data Transfers*, 17 July 2023, https://www.commerce.gov/node/5386

US Department of Justice Criminal Division, *CLOUD Act Resources*, updated on 14 October 2023, https://www.justice.gov/criminal/cloud-act-resources

Ursula von der Leyen, *Political Guidelines for the Next European Commission 2019-2024*, Luxembourg, Publications Office of the European Union, 2020, https://doi.org/10.2775/101756

ISSN 2610-9603 | ISBN 978-88-9368-344-9

ISSN 2610-9603 | ISBN 978-88-9368-344-9

IAI PAPERS 24 | 25 - SEPTEMBER 2024

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17 - I-00186 Rome, Italy
T +39 06 6976831
iai@iai.it
www.iai.it

Latest IAI PAPERS

Director: Riccardo Alcaro (r.alcaro@iai.it)