10

Data Protection and Artificial Intelligence

The European Union's Internal Approach and Its Promotion through Trade Agreements

Alan Hervé[*]

I INTRODUCTION

Europeans have only recently realized their weaknesses and the risk of remaining at the margins of the fourth industrial revolution[1] artificial intelligence (AI) is expected to bring about. Despite the existence of the single market, Europe industrial policy, including policy in the field of AI, still suffers from a lack of coordination and frequent duplications between member states. Moreover, investments in AI research and innovation remain limited when compared with Asia and North America.[2] As a result, European companies are in a weak position in terms of consumer application and online platforms, and industries are suffering from a structural disadvantage in the areas of data access, data processing and cloud-based infrastructures still essential for AI.

However, this gloomy overview calls for some nuance. The European Union (EU) and its member states are still well placed in the AI technological race, and the European economy benefits from several important assets, remaining not only an AI user but also, more critically, an AI producer. Europe[3] is still a key player in terms of research centers and innovative start-ups and is in a leading position in sectors such as robotics, service sectors, automotive, healthcare and computing infrastructure.

[*] I acknowledge the support of the European Commission through the European "Erasmus + Program", although all the opinions expressed in this chapter are personal. I warmly thank Thomas Streinz for his insightful comments on my preliminary draft. All mistakes that possibly remain in this final version are obviously mine.

[1] For a comprehensive study on the trade impact of the fourth industrial revolution, see M Rentzhog, "The Fourth Industrial Revolution: Changing Trade as We Know It" (*WITA*, 18 October 2019), https://perma.cc/5NLX-L7VA. See also the chapters by Aik Hoe Lim (Chapter 5) and Lisa Toohey (Chapter 17) in this volume.

[2] Overall, some 3.2 billion euros were invested in AI in Europe in 2016, compared with 12.1 billion in North America and 6.5 billion in Asia. European Commission, "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust", 2020 (hereinafter White Paper on AI).

[3] In this chapter, I will refer to "Europe" to describe the European Union and its member states.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

Perhaps more importantly, there is growing awareness in Europe that competition and the technological race for AI will be a matter of great significance for the future of the old continent's economy, its recovery after the COVID-19 pandemic and, broadly speaking, the strategic autonomy of the EU and its member states.

The 2020 European Commission White Paper on Artificial Intelligence illustrates a form of European awakening.[4] This strategic document insists on the necessity of better supporting AI research and innovation in order to strengthen European competitiveness. According to the Commission, Europe should particularly seize the opportunity of the "next data wave" to better position itself in the data-agile economy and become a world leader in AI.[5] The Commission makes a plea for a balanced combination of the economic dimension of AI and a values-based approach as the development of AI-related technologies and applications raises new ethical and legal questions.[6]

Profiling[7] and automated decision-making[8] are used in a wide range of sectors, including advertising, marketing, banking, finance, insurance and healthcare. Those processes are increasingly based on AI-related technologies, and the capabilities of big data analytics and machine learning.[9] They have enormous economic potential. However, services such as books, video games, music or newsfeeds might reduce consumer choice and produce inaccurate predictions.[10] An even more serious criticism is that they also can perpetuate stereotypes and discrimination bias.[11] Studies on this crucial issue are still rare because of a lack of access, as researchers often cannot access the proprietary algorithm.[12] In several European countries, including France, the opacity of algorithms used by the administration has become a political issue and has also provoked growing case law[13] and legislative changes.[14] Finally, as the European Commission recently observed, AI increases the possibility to track and

[4] See AI for Europe, COM(2018) 237 final, Brussels, 25.4.2018; and White Paper on AI, note 2 above, at 4. See also "Mission Letter: Commissioner-Designate for Internal Market" (2019), https://perma.cc/U7EW-C3MC.

[5] European Commission, AI White Paper, note 2 above; see also J Manyika, "10 Imperatives for Europe in the Age of AI and Automation" (2017), https://perma.cc/R5MP-DT82.

[6] FZ Borgesius, "Discrimination, Artificial Intelligence, and Algorithmic Decision Making" (2018), https://perma.cc/SHC7-WD5H.

[7] GDPR, Article 4(4).

[8] GDPR, Articles 15 and 22.

[9] 'Guidelines on Automated individual decision-making and profiling for the purpose of Regulation 2016/679, European Commission', October 2017.

[10] Ibid.

[11] See Z Obermeyer et al., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations" (2019) 336 *Science* 447.

[12] H. Ledford, *Nature* 574 (2019), 608–609.

[13] See, for instance, the ruling of the French constitutional court n° 2018–765 DC, "Loi relative à la protection des données personnelles", 12 June 2018. See also the Décret (executive order) n° 2017–330 du 14 mars 2017 "relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique", JO n° 64, 16 March 2017.

[14] One of the most controversial issues was the opacity of the algorithm used for the selection process at the public university. See C Villani and G Longuet, "Les algorithmes au service de l'action publique:

analyze people's habits. For example, there is the potential risk that AI may be used for mass state surveillance and also by employers to observe how their employees behave. By analyzing large amounts of data and identifying links among them, AI may also be used to retrace and deanonymize data about persons, creating new personal data protection risks.[15]

To summarize, the official European stance regarding AI combines a regulatory and an investment-oriented approach, with a twin objective of promoting AI and addressing the possible risks associated with this disruptive technology. This is indeed crucial as the public acceptance of AI in Europe is reliant on the conviction that it may benefit not only companies and decision-makers but also society as a whole. However, so far, especially when it comes to the data economy on which AI is largely based, public intervention in Europe has occurred through laws and regulations that are based on noneconomic considerations. The General Data Protection Regulation (GDPR)[16] is essential in this respect because it reflects how a human rights-based legal instrument might interfere with data-based economic principles. This 2016 regulation aims at enforcing a high standard of personal data protection that can limit the free flow of data, which is at the heart of the development of AI technologies.

Given the worldwide economic importance of the single market, the effects of this regulation are inevitably global. Many commentators rightly emphasized the extraterritorial effect of this European regulation, as a non-European company wishing to have access to the European market has no choice but to comply with the GDPR.[17] Moreover, the most recent generation of EU free trade agreements (FTAs) contains chapters on e-commerce and digital trade, under which the parties reaffirm the right to regulate domestically in order to achieve legitimate policy objectives, such as "public morals, social or consumer protection, [and] privacy and data protection". Under the latest EU proposals, the parties would recognize cross-border data flows, but they would also be able to "adopt and maintain the safeguards [they] deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data".[18]

The next section will present the growing debate on data protectionism (Section II). I will then study the EU's approach toward data protection and assess whether the set of internal and international legal provisions promoted by the EU effectively

le cas du portail admission post-bac–Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques" (2018), https://perma.cc/U9R4-ZT67.

[15] See White Paper on AI, note 2 above, at 12.

[16] Regulation (EU) 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88.

[17] GDPR, Article 83.

[18] See "EU Proposal on Digital Trade for the EU-Australia FTA" (2018), https://perma.cc/2KQ8-F9HF.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

translates into a meaningful balance between trade, innovation and ethical values (Section III). I will also describe the birth of European trade diplomacy in the field of digital trade, focusing the analysis on the most recent EU FTAs' provisions and proposals. I will compare them with recent US-led trade agreements, such as the Trans-Pacific Partnership (TPP) and the United States-Mexico-Canada Agreement (USMCA), to assess whether the EU's approach constitutes a model for future plurilateral or multilateral trade agreements (Section IV). In conclusion, I will assess whether the American and European approaches are reconcilable or destined to diverge given the opposing political and economic interests they translate.

II DATA PROTECTION OR DATA PROTECTIONISM?

Data has often been described as a contemporary raw material, a sort of postindustrial oil, and its free flow as the necessary condition for the convergence between globalization and digitalization. Data is at the heart of the functioning of AI, which is in turn the most important application of a data economy. The development of AI relies on the availability of data, and its value increases with detailed and precise information, including private information.[19] The availability and enhancement of data are crucial for the development of technologies, such as machine learning and deep learning, and offer a decisive competitive edge to companies involved in the global competition for AI.[20] Moreover, access to data is an absolute necessity for the emergence and development of a national and autonomous AI industry.[21] Not surprisingly, given the growing economic and political importance of data, governments and policy-makers are increasingly trying to assert control over global data flows. This makes sense as data, and in particular private data, is more and more presented as a highly political issue that has for too long been ignored in the public debate.[22]

The current move toward digital globalization could be threatened by three types of policies: new protectionist barriers, divergent standards surrounding data privacy and requirements on data localization.[23] Data localization has also been

[19] Scholars have tried to compartmentalize data into different categories such as personal data, public data, company data, business data, etc. In practice, however, it appears to be difficult to apply different legal instruments based on the nature of the data. Cross-border data transfers mostly cover personal data, which has both a private value and an economic value. See N Mishra, "Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows" (2019) 52 *Vanderbilt Journal of Transnational Law* 463, at 472–473; and S. Yakovleva, "Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?" (2018) 17 *World Trade Review* 477.

[20] C. Villani et al., "Donner Un Sens à l'Intelligence Artificielle. Pour Une Stratégie National et Européenne" (2018), https://perma.cc/SLC9-AMNZ.

[21] European Commission, White Paper on AI, note 2 above, at 3.

[22] See S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30 *Journal of Information Technology* 75.

[23] See J Manyika et al., "Digital Globalization: The New Era of Global Flows" (2016), https://perma.cc/3XCW-4U86.

depicted as "data protectionism" and a new form of nationalism,[24] or even anti-Americanism,[25] whereas others have advocated for a "digital sovereignty" that would imply the state's power to regulate, limit or even prohibit the free flow of data.[26] Many countries are indeed subject to internal tensions between supporters of data openness as a catalyst for trade and technological development and those who promote comprehensive data protection in order to defend digital sovereignty as a prerequisite of national sovereignty. Old concepts and notions of international law, such as (digital) self-determination, (data) colonization, reterritorialization of data and (digital) emancipation, are also mobilized when it comes to justifying states' "right to regulate" data. However, those general concepts often appear inadequate given the intrinsic nature of data flows and Internet protocol, which tend to blur the distinction between the global and the local. Data flows somehow render obsolete the traditional considerations of geographical boundaries and cross-border control that characterize classical international law.[27]

Neha Mishra has thoroughly described different types of data-restrictive measures. State control can intervene using the physical infrastructures through which Internet traffic is exchanged, a local routing requirement and a variety of cross-border data flow restrictions, such as data localization measures or conditional restrictions imposed on the recipient country or the controller/processor.[28] Primary policy goals may justify those restrictions on the grounds of public order and moral or cultural issues. In Europe, the rationale behind the restrictions on the cross-border of data transfer and AI has been primarily addressed through the angle of data protection – that is, the defense and protection of privacy – as one of the most fundamental human rights.

This narrative extends well beyond the sole economic protection of European interests and has the enormous advantage of conciliating protectionist and nonprotectionist voices in Europe. It contrasts and conflicts with an American narrative based on freedom and technological progress, where free data flows are a prerequisite for an open and nondiscriminatory digitalized economy.

[24] A Chander and UP Lê, "Data Nationalism" (2015) 64 *Emory Law Journal* 677.

[25] See "The Rise of Digital Protectionism" (Council on Foreign Relations, 18 October 2017), https://perma.cc/P4H2-7BFV</int_i. The participants in this workshop considered that Chinese measures on data localization reflected China's "authoritarian" and "mercantilist" model, whereas "Europe's digital protectionism" is described as "in line with Brussels' legalistic, top-down, heavily regulated approach to economic policy".

[26] This claim for sovereignty is in reality as old as the existence of a public debate on data flows. See C Kuner, "Data Nationalism and Its Discontent" (2015) 64 *Emory Law Journal* 2089. See also S Aaronson, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights and National Security" (2015) 14(4) *World Trade Law Review* 671.

[27] See Mishra, note 19 above, at 473.

[28] Ibid., at 474–477.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

III THE EUROPEAN LEGAL DATA ECOSYSTEM AND ITS IMPACTS ON ARTIFICIAL INTELLIGENCE AND INTERNATIONAL DATA FLOWS

The European Legal Framework on data, and in particular on data protection, is nothing new in the EU. It can be explained in the first place by internal European factors. European member states started to adopt their own law on the protection of personal information decades ago,[29] on the grounds of the protection of fundamental rights, and in particular the right to privacy, protected under their national Constitution, the European Convention on Human Rights and the European Charter of Human Rights, which forms part of current primary EU law. Therefore, EU institutions recognized early the need to harmonize their legislation in order to combine the unity of the single market and human rights considerations already reflected in member states' legislation. It explains why, while some international standards, namely those of the Organisation for Economic Co-operation and Development (OECD)[30] and Asia-Pacific Economic Cooperation (APEC),[31] emphasize the economic component of personal data, the EU's legal protection has been adopted and developed under a human rights-based approach toward personal data.[32]

The 1995 European Directive was the first attempt to harmonize the protection of fundamental rights and freedoms of natural persons with respect to processing activities, and to ensure the free flow of data between member states.[33] However, a growing risk of fragmentation in the implementation of data protection across the EU and legal uncertainty justified the adoption of a new instrument that took the form of a Regulation, which is supposed to provide stronger uniformity in terms of application within the twenty-seven member states.[34]

The GDPR also represents a regulatory response to a geopolitical challenge initiated by the United States and its digital economies to the rest of the world. From a political perspective, the Snowden case and the revelation of the massive surveillance organized by American agencies provoked a strong reaction among European public opinion, including within countries that had recently experimented with authoritarian regimes (such as the former East Germany and

[29] For instance, the French legislation "informatique et liberté" was adopted in January 1978. See Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[30] See "The OECD Privacy Framework" (2013), https://perma.cc/BC7W-B6VW, and also its explanatory Memorandum.

[31] See "APEC Privacy Framework" (2015), https://perma.cc/VBW5-4ZCL.

[32] Yakovleva, note 19 above.

[33] 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, OJ L 281, 23.11.1995 (hereinafter Data Protection Directive).

[34] Despite this general assumption, one can observe that the GDPR leaves in practice some discretion to national authorities, in particular when it comes to the procedural enforcement of the substantive rights granted under this regulation.

Poland).[35] The Facebook-Cambridge Analytica scandal further demonstrated that the freedom of millions of Europeans and their democracies was at stake and could be threatened by the digital hegemony of American tech companies with commercial interests. The demand for data protection against free and uncontrolled flows of data has also been encouraged by the progressive awareness of the economic and technological consequences of free data flows, as European companies appeared to be increasingly outpaced by their American rivals, especially in the field of AI. In parallel, in a spectacular ruling in 2015, the European Court of Justice annulled a decision of the European Commission, under which the United States was until then considered to be providing a sufficient level of protection for personal data transferred to US territory (under the so-called safe harbor agreement).[36]

The GDPR has been both praised and criticized, within and outside of Europe. Still, it remains to a certain extent a legal revolution in the field of data regulation, not so much because of its content – it is not, after all, the first legal framework to deal with algorithms and data processing – but more because of the political message this legislation sends to the European public and the rest of the world.[37] Through the adoption of this Regulation in 2016, the EU has chosen to promote high standards for data protection. Every single European and non-European company that is willing to process European data, including those developing AI, must comply with the GDPR.[38]

A *European Data Protection's Regulation and Artificial Intelligence*

The GDPR regulates the processing of personal data; that is, any information relating to a directly or indirectly identified or identifiable natural person ("data subjects"). This legislation deals with AI on many levels.[39] First, it contains a very broad definition of "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means".[40]

[35] The Commission proposed the first version of the future GDPR in January 2012. The discussion progressed very slowly until 2014 and the revelations of Edward Snowden in 2014. The GDPR was finally adopted in April 2016.

[36] ECJ, 6 October 2015, Judgment in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650.

[37] Even though Europe is not the sole region that adopted a data privacy legislation, according to the United Nations Conference on Trade and Development (UNCTAD), 66 percent of countries worldwide have a data protection law. See "Data Protection and Privacy Legislation Worldwide" (2020), https://perma.cc/BCP3-C2BA.

[38] Compare GDPR Article 3(2).

[39] For a comprehensive review of the GDPR, see PM Schwartz, "Global Data Privacy: The EU Way" (2019) 94 *NYU Law Review* 771.

[40] GDPR, Article 4(4).

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

It also regulates the conditions under which "personal data"[41] can be collected, retained, processed and used by AI. The GDPR is built around the concept of lawful processing of data,[42] meaning that personal data *cannot* be processed without obtaining individual consent or without entering into a set of limited categories defined under the Regulation.[43] That is a crucial difference between current American federal and state laws, which are based on the presumption that data processing is lawful unless it is explicitly prohibited by the authorities under specific legislation.[44]

Under the GDPR, processing of personal data is subject to the lawfulness, fairness and transparency principles.[45] The Regulation also contains specific transparency requirements surrounding the use of automated decision-making, namely the obligation to inform about the existence of such decisions, and to provide meaningful information and explain its significance and the envisaged consequences of the processing to individuals.[46] The right to obtain information also covers the rationale of the algorithms, therefore limiting their opacity.[47] Individuals have the right to object to automated individual decision-making, including the use of data for marketing purposes.[48] The data subject has the right to not be subject to a decision based solely on automated decision-making when it produces legal effects that can significantly affect individuals.[49] Consent to the transfer of data is also carefully and strictly defined by the Regulation, which states that it should be given by a clear affirmative act from the natural person and establishes the principles of responsibility and liability of the controller and the processor for any processing of personal data.[50] Stringent forms of consent are required under certain specific circumstances, such as automated decision-making, where explicit consent is needed.[51]

Therefore, under the GDPR, a controller that will use data collected for profiling one of its clients and identifying its behavior (for instance, in the sector of insurance)

[41] The GDPR only deals with personal data. Nonpersonal data is addressed by Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of nonpersonal data in the European Union, OJ L 303, 28.11.2018, at 59–68.

[42] GDPR, Article 6.

[43] Compare GDPR, Article 6(1).

[44] A Chander et al., "Catalyzing Privacy Law" (2019), https://scholarship.law.georgetown.edu/facpub/2190.

[45] GDPR, Article 5(1)(a).

[46] GDPR, Article 13.2.

[47] GDPR, Article 15.1. The contours of this right are, however, controversial. Some authors argue it amounts to a right to explanation. See AD Selbst and J Powles, "Meaningful Information and the Right to Explanation" (2017) 7(4) *International Data Privacy Law*, at 233.

[48] GDPR, Article 21.

[49] GDPR, Article 22. Exceptions remain, for instance, if they are entering into a contract based on the data subject's explicit consent, or if they are authorized under the member states' laws. Article 22(2)(c) GDPR.

[50] GDPR, Article 24.

[51] GDPR, Article 22(1)(c). This is also supported by recital 71 of the GDPR.

must ensure that this type of processing relies on a lawful basis. Moreover, the controller must provide the data subject with information about the data collected. Finally, the data subject may object to the legitimacy of the profiling.

Another illustration of the interference between AI technologies and GDPR is the requirements and limitations imposed on the use of biometric data[52] for remote identification, for instance through facial recognition. The GDPR prohibits the process of biometric data "for the purpose of uniquely identifying a natural person" unless the data subject has given explicit consent.[53] Other limitations to this prohibition are exhaustively delineated, such as the "protection of the vital interests" of the data subject or other natural persons, or for reasons of "substantial public interest". Most of those limited biometric identification purposes will have to be fulfilled according to a necessity and a proportionality test and are subject to judicial law review.[54]

B *Transatlantic Regulatory Competition*

Despite its limitations and imperfections, the GDPR remains as a piece of legislation that aims to rightfully balance fundamental rights considerations with technological, economic and policy considerations in accordance with European values and standards. In contrast, US law surrounding the data privacy legal framework does not rely on human rights but, rather, on consumer protection, where the individual is supposed to benefit from a bargain with the business in exchange for its personal information (the so-called transactional approach).[55] Moreover, in contrast with Europe's unified and largely centralized legislation, the American model for data protection has primarily been based on autoregulation and a sectoral regulation approach, at least until the 2018 adoption of the California Consumer Privacy Act (CCPA).[56]

This state legislation partially resembles the GDPR. First, the CCPA is the first data protection statute that is not narrowly sectoral.[57] It defines "personal information" in a way that seems in practice equivalent to the GDPR's personal data definition.[58] Personal information is also partially relevant to AI (such as biometric data, geolocalization and Internet, or other electronic network information). It also includes a broad definition of processing, which can include automated decision-

[52] Compare the definition of biometric data in GDPR, Article 4 (14).
[53] GDPR, Article 9.1.
[54] GDPR, Article 9.2.
[55] See Chander et al., note 44 above, at 13.
[56] The CCPA entered into force in January 2020. SB-1121 California Consumer Privacy Act of 2018 (hereinafter CCPA).
[57] However, at the federal level, sensitive data that are considered noncommercial also benefit from strong protection. That is the case, in particular, for data collected by hospitals or the banking sector. See, for instance, the Health Insurance Portability and Accountability Act, 45 C.F.R. § Parts 160, 162 and 164.
[58] See CCPA SEC.9 (o).

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

making.[59] Echoing the GDPR's transparency requirements, the CCPA provides a right of information, under which a consumer has the right to request that a business that collects consumers' personal information disclose to that consumer the categories and specific pieces of personal information collected.[60] This right of disclosure is particularly significant.[61] The CCPA also contains a right to opt out and deny the possibility for a business to use its personal information.[62]

Despite those similarities, important differences remain between the two statutes. Concretely, under the CCPA's transactional approach, the right to opt out cannot be opposed if it is necessary to business or service providers to complete the transaction for which the personal information was collected or to enable solely internal uses that are reasonably aligned with the expectations of the consumer's relationship with the business.[63] Moreover, whereas the GDPR rests on the principle of the "lawful processing of data",[64] the CCPA does not require processing to be lawful, implying that data collection, use and disclosure is allowed unless it is explicitly forbidden. Whereas the GDPR requires some specific forms of consent related to sensitive data and limits individual automated decision-making, the CCPA "does nothing to enable individuals to refuse to give companies their data in the first place".[65] Another striking difference is related to the consumer's right not to be discriminated against under the CCPA if he or she decides to exercise the right to seek information or the right to opt out. The effect of this nondiscrimination principle seems tenuous as, in those circumstances, a business is not prohibited from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer.[66] This is typically the result of a consumer protection-based approach, which in reality tolerates and admits discrimination (here, the price or the quality of the service provided), and a human rights-based approach that is much more reluctant to admit economic differentiations among individuals to whom those fundamental rights are addressed.

This brief comparison between the GDPR and the CCPA is not meant to suggest that one legislative model is intrinsically superior, more efficient, more legitimate or more progressive than the other. Both statutes merely translate ontological discrepancies between the European and American legal conceptions and policy choices. However, the conflict between those two models is inevitable when considering the current state of cross-border data flows. Not surprisingly, the question of extraterritoriality was crucial during the GDPR's drafting.[67] Even though the Regulation is based on the necessity of establishing a single digital market, under which data

59 See CCPA SEC.9 (q).
60 CCPA SEC.1A. See further Chander et al., note 44 above, at 14–16.
61 CCPA SEC.3 (a).
62 CCPA SEC.2 (a).
63 CCPA SEC.2 (d). Compare GDPR Article 22(2)(a).
64 GDPR Article 6(1). Chander et al., note 44 above, at 19.
65 Ibid., at 20.
66 CCPA SEC.6 (a)(2).
67 See in particular D. Bernet's insightful documentary *Democracy: Im Rausch der Daten* (2015).

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

protection and fundamental EU rights are equally guaranteed, its extraterritorial effects are expressly recognized as the GDPR applies "in the context of the activities of an establishment of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union or not*" and "to the processing of personal data subjects who are in the Union by a controller or processor *not established in the Union*".[68] The extraterritorial effects of the GDPR and, more broadly, of the EU's legal framework are undeniable given the importance of the single EU market.[69] Extraterritoriality should be understood as a kind of "effet utile" of the Regulation, as most of the data processors and controllers are currently located outside the EU's territory. The EU's effort would in practice be doomed if personal data protection were to be limited to the EU borders.[70]

The European legislator admits that flows of personal data to and from countries outside the EU are necessary for the expansion of international trade.[71] Yet, international data transfers must not undermine the level of data protection and are consequently subject to the Regulation's provisions. Data transfer to third countries is expressly prohibited under the GDPR unless it is expressly authorized thanks to one of the legal bases established under the Regulation.[72] The European Commission may decide under the GDPR that a third country offers an adequate level of data protection and allow transfers of personal data to that third country without the need to obtain specific authorization.[73] However, such a decision can also be revoked.[74] In the absence of an adequacy decision, the transfer may be authorized when it is accompanied by "appropriate safeguards", which can take the form of binding corporate rules[75] or a contract between the exporter and the importer of the data, containing standard protection clauses adopted by the European Commission.[76] Even in the absence of an adequacy decision or appropriate safeguards, data transfer to third countries is allowed under the GDPR, in particular on the consent of the data subject, and if the transfer is necessary for the performance of a contract.[77]

[68] GDPR, Article 3.

[69] See A Bradford, *The Brussels Effect: How the European Union Rules the World* (New York, Oxford University Press, 2020). For a distinction between the so-called Delaware Effect, California Effect and Brussels Effect, see Chander et al., note 44 above.

[70] Schwartz, note 39 above, at 11. For a discussion of the GDPR's limits see ECJ, 24 September 2018, Judgment in Case C-507/17, *Google LLC, v. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772.

[71] GDPR, Recital 201.

[72] GDPR, Article 44.

[73] This adequacy requirement of the data protection level in the foreign jurisdiction was already in place in the Data Protection Directive, note 33 above. Before its adoption, member states had their own adequacy requirements. Schwartz, note 39 above, at 11–12.

[74] GDPR, Articles 44 and 45.

[75] Defined as internal corporate rules for data transfers within multinational organizations.

[76] GDPR Articles 46 and 47.

[77] GDPR Article 49.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

Under the current regime, the EU Commission adopted a set of adequacy findings with select third countries, such as Japan, in February 2019.[78] The European Commission also commenced adequacy negotiations with Latin American countries (Chile and Brazil) and Asiatic countries (Korea, India, Indonesia, Taiwan), as well as the European Eastern and Southern neighborhoods, and is actively promoting the creation of national instruments similar to the GDPR.[79] Moreover, in July 2016, the European Commission found that the EU-US Privacy Shield ensures an adequate level of protection for personal data that has been transferred from the EU to organizations in the USA, demonstrating regard for, inter alia, safeguards surrounding access to the transferred data by the United States' intelligence services.[80] More than 5,300 companies have been certified by the US Department of Commerce in charge of monitoring compliance with a set of common data privacy principles under the Privacy Shield, which is annually and publicly reviewed by the Commission.[81] The Privacy Shield seemed to demonstrate that despite profound divergence between European and American approaches to data protection, there was still room for transatlantic cooperation and mutual recognition. However, in mid-July 2020, the European Court of Justice (ECJ) concluded that the Commission's Privacy Shield decision was invalid as it disregarded European fundamental rights.[82] As the Court recalled, the Commission must only authorize the transfer of personal data to a third country if it provides "a level of protection of fundamental rights and freedoms essentially equivalent to that guaranteed within the European".[83] The ECJ found lacunae in judicial protections for European data subjects against several US intelligence programs.[84]

The question of data transfer between the EU and UK after Brexit is one of the many hot topics that should be dealt with in a future EU/UK trade agreement, and it is a perfect example of the problematic nature of the GDPR's application to EU third countries with closed economic ties. The October 2019 political declaration setting out the framework for the future relationship between the two parties contains a specific paragraph on digital trade that addresses the question of data

[78] The European adequacy decision came after Japanese internal reforms on data privacy law, in particular the extensive 2015 amendment to Japan's Act on the Protection of Personal Information (APPI). See Schwartz, note 39 above, at 14–16. See the Commission Implementing Decision (EU) 2019/419 of 23 January 2019, OJ L 76, 19.3.2019. This decision scrutinizes the Japanese legal framework concerning data protection.

[79] Data protection rules as a trust-enabler in the EU and beyond – taking stock, COM(2019) 374 final, July 2019. See also the list of adequacy decisions at https://perma.cc/VA6X-ZQ3T.

[80] The Privacy Shield had to be negotiated after the European Court of Justice found that a former EU-US safe harbor arrangement was incompatible with EU law. See *Maximillian Schrems v. Data Protection Commissioner*, note 35 above.

[81] "Privacy Shield Framework", https://perma.cc/RTZ2-UAT5.

[82] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems*, 16.07.2020.

[83] Ibid., at part 94.

[84] The adequacy decision being annulled, future data transfer will, however, remain possible under GDPR Article 49.

protection. It says that future provisions on digital trade "should . . . facilitate cross-border data flows and address unjustified data localisation requirements, noting that this facilitation will not affect the Parties' personal data protection rules".[85] However, in June 2020, six months after Brexit, the Commission was still uncertain regarding a future UK adequacy assessment because of a lack of specific data protection commitment in the UK. Moreover, the British government indicated that it wanted to develop a separate and independent data protection policy.[86] One of the EU's main concerns is that through bilateral agreements concluded between the UK and the USA, data belonging to EU citizens could be "siphoned off" to the United States.[87]

The issue of compatibility between European privacy rules and the Chinese legal framework is also a growing matter of concern for Europeans. China applies much stricter data border control on the grounds of national security interests. For instance, the 2017 Chinese law on cybersecurity provides that companies dealing with critical infrastructures of information, such as communications services, transport, water, finances, public services energy and others, have an obligation to store their data in the Chinese territory. Such a broad definition can potentially affect all companies, depending on the will of Chinese authorities, who also have broad access to personal information content on the grounds of national security.[88] However, Chinese attitudes regarding privacy protection are not monolithic. According to Samm Sacks, "[t]here is a tug of war within China between those advocating for greater data privacy protections and those pushing for the development of fields like AI and big data, with no accompanying limits on how data is used". This expert even describes a growing convergence between the European and Chinese approaches in data protection regimes, leading the USA to be more isolated and American companies to be more reactive.[89] However, based on the model of the recent conflict between European data privacy rules and US tech companies' practices, emerging cases that shed new light on data protection regulatory divergence between China and the EU are inevitable.[90]

Fragmentation and market barriers are emerging around requirements for privacy and data flows across borders. Can this fragmentation be limited through international

[85] See "Revised Political Declaration Setting Out Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom as Agreed at Negotiators' Level" (17 October 2019), https://perma.cc/5Y4S-XBQU.

[86] See Boris Johnson's Government written statement on the UK/EU relationship made on 3 February 2020.

[87] See, for instance, the Access to Electronic Data for the Purpose of Countering Serious Crime Agreement signed between the UK and the USA in October 2019.

[88] S Livingstone, "China Sets to Expand Data Localization and Security Services Requirements" (IAPP, 25 April 2017), https://perma.cc/3R5N-CL4A.

[89] See S Sacks, "New China Data Privacy Standard Looks More Far-Reaching Than GDPR" (Center for Strategic and International Studies, 29 January 2018), https://perma.cc/A6AH-8EYX.

[90] See German Labour Court ruling concerning Huawei, "Arbeitsgericht Düsseldorf, 9 Ca 6557/18" (Justiz-Online, 5 March 2020), https://perma.cc/9FEV-2TGX.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

trade law? What is the EU's position on international data flows and data protection in the context of its trade policy? Can and should European trade agreements become an efficient way to promote the GDPR's privacy approach?

IV THE BIRTH OF EUROPEAN DIGITAL TRADE DIPLOMACY

Not surprisingly, given its imprecise nature, AI is not covered as such by trade agreements, although AI technologies that combine data, algorithms and computing power can be affected by trade commitments in the field of goods and services. In this section, I will focus on the issue of the trade dimension of cross-border data flows, given its strategic relevance to AI applications. Although data cannot be assimilated to traditional goods or services, trade rules matter with regard to data in multiple ways.[91] As I have already noted, even though regulating data flows on national boundaries might seem counterintuitive and inefficient,[92] states and public authorities are tempted to regain or maintain control of data flows for many reasons, ranging from national security to data protection to economic protectionism. A trade agreement is one international public law instrument that might constitute a legal basis to promote cross-border data control or, on the contrary, the free flow of data principle.

A *A Limited Multilateral Framework*

Despite recent developments, digital trade rules currently remain limited, both at the multilateral and the bilateral level. World Trade Organization (WTO) disciplines do not directly confront the problematic nature of digital trade or AI, even though the WTO officially recognizes that AI, together with blockchain and the Internet of Things, is one of the new disruptive technologies that could have a major impact on trade costs and international trade.[93] Mira Burri has, however, described how WTO general nondiscrimination principles – Most Favorable Nation Treatment and National Treatment – could potentially have an impact on the members' rules and practices regarding digital trade, as well as more specific WTO agreements, especially the General Agreement on Trade in Services (GATS).[94] She notes that WTO members have made far-reaching commitments under the GATS. The EU in particular has committed to data processing services,

[91] See Mishra, note 19 above; M Burri, "The Regulation of Data Flows Through Trade Agreements" (2017) 51 *UC Davis Law Review* 407, at 468.

[92] Mishra, note 19 above.

[93] See World Trade Organization, "World Trade Report 2018: The Future of World Trade – How Digital Technologies Are Transforming Global Commerce" (2018), https://perma.cc/S9AM-A26P; D Mitchell and N Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute" (2019) 22(3) *Journal of International Economic Law* 389.

[94] M Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 *UC Davis Law Review* 65.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

database services and other computing services.[95] These commitments might prohibit new measures with regard to search engines that limit market access or discriminate against foreign companies, as they should be considered data processing services. Localization requirements with regard to computer and related services would also be prima facie GATS-inconsistent, but could well be justified under the agreement's general exceptions.[96]

Despite a few updates, such as the Information Technology Agreement, WTO members have failed, as in other fields, to renovate and adapt proper WTO disciplines to strategic issues, such as digital trade and AI. The current plurilateral negotiations on e-commerce, which involve seventy-nine members including China, Japan, the USA and the EU and its member states, might represent a new opportunity to address these issues.[97] However, given the current state of the WTO, such evolution remains, at present, hazardous.[98] So far, the most relevant provisions on digital trade are those negotiated within the bilateral or plurilateral trade deals, beginning with the TPP.[99]

Recent developments in EU digital trade diplomacy can be seen as a reaction to the United States' willingness to develop an offensive normative strategy whose basic aim is to serve its big tech companies' economic interests and to limit cross-border restrictions based on data privacy protection as much as possible.

B *The US Approach to Digital Trade Diplomacy*

The United States' free trade agreement (FTA) provisions on digital trade are the result of the Digital Agenda that was endorsed in the early 2000s. Several US trade agreements containing provisions on e-commerce have been concluded by different American administrations over the last two decades.[100] In 2015, the United States Trade Representative described the TPP as "the most ambitious and visionary

[95] Ibid., at 84.

[96] Ibid. See also the way the WTO Appellate Body interpreted GATS article XIV in *US – Gambling* (WT/DS285/ABR, 7 April 2005).

[97] See the WTO Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019. See also Henry Gao's Chapter 15 in this volume.

[98] It can even be traced back to the Clinton administration's framework for global electronic commerce. See T Streinz, "Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy," in B Kingsbury et al. (eds), *Megaregulation Contested Global Economic Ordering After TPP* (Oxford, Oxford University Press, 2019).

[99] Ibid.

[100] See the FTAs concluded with Australia (2002), Singapore (2003), Bahrain (2004), Chile (2004), the central American countries (2004), Morocco (2006), Oman (2009), Peru (2009), Panama (2012), Colombia (2012) and especially Korea (2012), which was, until the TPP, the most advanced FTA on digital trade. See S Wunsch-Vincent and A Hold, "Toward Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Agreements", in M Burri and T Cottier (eds), *Trade Governance in the Digital Age* (Cambridge, Cambridge University Press, 2011).

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

internet agreement ever attempted".[101] The TPP provisions relate to digital trade[102] in various respects, including, inter alia, nondiscriminatory treatment of digital products,[103] a specific ban of custom duties on electronic transmission[104] and free supply of cross-border digital services.[105] More specifically, despite recognizing the rights of the parties to develop their own regulatory requirements concerning the transfer of information by electronic means, the agreement prohibits the limitation of cross-border transfer of information by electronic means, including personal information.[106] Additionally, under the TPP, "no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory".[107] US tech companies were deeply satisfied with the content of the agreement.[108]

However, the TPP drafters did not ignore the problematic nature of personal information protections. Indeed, the text of this agreement recognized the economic and social benefits of protecting the personal information of users of electronic commerce.[109] It even indicated that each party *shall* adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce, therefore admitting the possibility of following different legal approaches. However, each party should adopt instruments to promote compatibility between the different legal frameworks,[110] and the agreement's wording is relatively strong on the nondiscriminatory practices in terms of user protections.

The GDPR was still under discussion when the TPP was concluded. However, there is room for debate concerning the possible compatibility of the European legislation and this US trade treaty. As with the WTO compatibility test, the main issue concerns the possible discriminatory nature of the GDPR, which in practice is arguable. This doubt certainly constituted an incentive for the EU to elaborate upon and promote its own template on digital trade, in order to ensure that its new

[101] The Bipartisan Congressional Trade Priorities and Accountability Act of 2015, P.L. 114–26 sec. 102 (b)(6) adopted by the US Congress included precise negotiations objectives for digital trade in goods and services and cross-border data flows.

[102] See TPP chapter 14 on "Electronic Commerce".

[103] TPP, Article 14.4.

[104] TPP, Article 14.3.

[105] Cross-border service provisions of US FTAs have always been very liberal as they rely on a negative approach, meaning that a cross-border service should be liberalized unless the contracting parties expressly restrict it. See TPP, Article 14.2.4.

[106] TPP, Article 14.11.2.

[107] TPP, Article 14.13. However, such a provision is subject to limitations on the grounds of legitimate public policy objectives, provided that they are not applied in a discriminatory and disproportionate manner. TPP, Article 14.8.

[108] See "IBM Comments on U.S. Review of Trade Agreements" (THINKPolicy Blog, 31 July 2017), https://perma.cc/4GGR-YZVC.

[109] TPP, Article 14.8.1.

[110] Both autonomous instruments and mutually agreed-upon solutions are permitted, which seems to echo the GDPR mechanisms described.

legislation wouldn't be legally challenged by its trade partners, including the US administration.

Just like the TPP, the USMCA contains several provisions that address digital trade, including a specific chapter on this issue.[111] It also prohibits custom duties in connection with digital products[112] and protects source code.[113] The prohibition of any cross-border transfer or information restriction is subject to strong wording, as the agreement explicitly provides that "[n]o Party *shall* prohibit or restrict the cross border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person".[114] Yet, the USMCA admits the economic and social benefits of protecting the personal information of users of digital trade and the relevance of an internal legal framework for the protection of this information.[115] However, the conventional compatibility of internal regulations that would limit data collection relies on a necessity and proportionality test and a nondiscrimination requirement. In any case, the burden of proving compatibility will undoubtedly fall on the party that limited data transfer in the first place, even though it did so on the grounds of legitimate policy objectives. Under these circumstances, the legality of GDPR-style legislation would probably be even harder to argue than under the former TPP.

C *The European Union's Response to the American Trade Regulatory Challenge*

Before studying the precise content of existing EU agreements and proposals on digital trade, one should bear in mind that European trade policy is currently subject to strong internal tensions. Trade topics have become increasingly politicized in recent years, especially in the context of the Comprehensive Economic and Trade Agreement (CETA) and Transatlantic Trade and Investment Partnership (TTIP) negotiations. It is not only member states, through the Council, and the European Parliament – which has obtained, after the Lisbon Treaty, the power to conclude trade agreements together with the Council – that have placed pressure on the Commission. Pressure has also come from European civil society, with movements organized at the state and the EU level.[116] As a result, the idea that trade deals should no longer be a topic for specialists and be subject to close political scrutiny is gaining ground in Europe. As a response, the capacity of trade agreements to better regulate international trade is now part of the current Commission's narrative to advocate for

[111] The name of the USMCA chapter is now "digital trade", which may sound more precise than the TPP's "electronic commerce" language.
[112] USMCA, Article 19.3.
[113] USMCA, Article 19.16.1.
[114] USMCA, Article 19.11.1.
[115] USMCA, Article 19.8.
[116] See Stop-TTIP European Citizens' Initiative, registered in July 2017, Commission registration number: ECI(2017)000008.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

the necessity of its new FTA generation,[117] in line with European primary law provisions that connect trade with nontrade policy objectives.[118] The most recent generation of EU FTAs incorporate a right to regulate, which is reflected in several provisions, in particular in the context of the sustainable development[119] and investment chapters.[120] More recently, the EU also showed a willingness to include a right to regulate in the digital chapter's provisions.[121] Paradoxically, the recall of the state power to regulate is the prerequisite of stronger trade liberalization[122] and, more broadly, a way in which to legitimize the extension of trade rules.

Older trade agreements, meaning those concluded before 2009, when the Lisbon Treaty entered into force, remained practically silent on the issue of digital trade or electronic commerce. The EU-Chile (2002) trade agreement is probably the first FTA that contains references to e-commerce, probably under the influence of the US-Chile FTA concluded during the same period. However, the commitments were limited as they refer to vague cooperation in this domain.[123] Moreover, the service liberalization was strictly contained within the limits of the positive list-based approach of the former generation of European FTAs.[124] The EU-Korea FTA of 2011 contains more precise provisions on data flows, yet it is limited to specific sectors.[125] For instance, Article 7.43 of this agreement, titled "data processing", is part of a broader subsection of the agreement addressing financial services. The provision encourages free movement of data. Yet, it also contains a safeguard justified by the protection of privacy. Moreover, the parties "agree that the development of electronic commerce must be fully compatible with the international standards of data protection, in order to ensure the confidence of users of electronic commerce". Finally, under this agreement, the cross-border flow of supplies can be limited by the necessity to secure compliance with (internal) laws or regulations, among which is

[117] See, for instance, the Commission's Communication *Trade for All*, COM (2015) 497 final, 14.10 and A Hervé, "The European Union and Its Model to Regulate International Trade Relations" (2020) Schuman Foundation Paper, European Issue n° 554, https://perma.cc/B43D-37P2.

[118] Compare TFEU Article 207.

[119] See JEFTA (Japan/EU FTA, OJ L 330, 27.12.2018, 3–899), Article 16.2.

[120] See CETA, Article 8.9 (in the context of the investment protection's chapter); see also the EU-Canada Joint Interpretative Instrument where both parties "recognise the importance of the right to regulate in the public interest" (OJ L 11, 14.1.2017, 3–8).

[121] See the recently concluded EU/Mexico FTA chapter on digital trade.

[122] This paradox of a deeper liberalization accompanied by measures involving a stronger state and administrative control has been famously pictured by Michel Foucault through his concept of "biopower" and "biopolitics". See M Foucault, *The Birth of Biopolitics: Lectures at the College de France 1978–1979* (New York, Palgrave Macmillan, 2008).

[123] Compare Article 104 of the EU-Chile Association Agreement, OJ L 352, 30.12.2002, 3–1450.

[124] See Burri, note 91 above, at 426. However, after CETA, the EU accepted to conclude FTAs based on a negative service liberalization approach. That is the case of the JEFTA, although the liberalization remains subject to a long list of exceptions.

[125] This evolution might be explained by the existence of commitments on e-commerce in the KORUS FTA, signed in 2007 (see KORUS chapter 15 on Electronic Commerce). However, KORUS Article 15.8 uses soft wording regarding free data flows ("the Parties *shall endeavor to refrain* from imposing or maintaining unnecessary barriers to electronic information flows across borders").

the protection of the privacy of individuals.[126] Although limited to specific sectors, those provisions demonstrate that the EU was aware of the potential effect of data protection on trade long before the adoption of the GDPR.[127]

This sectoral approach has been followed by the EU and its partners in more recent trade agreements, such as the CETA between the EU and Canada, which was concluded in 2014.[128] Chapter 16 of the CETA agreement deals expressly with e-commerce. It prohibits the imposition of customs duties, fees or charges on deliveries transmitted by electronic means.[129] It also states that "[e]ach Party *should* adopt or maintain laws, regulations or administrative measures for the protection of *personal information of users* engaged in electronic commerce and, when doing so, *shall* take into due consideration international standards of data protection of relevant international organizations of which both Parties are a member".[130] However, the CETA also contains another innovative and broader exception clause based on data protection. Article 28.3 addresses the general exception to the agreement, and provides that several chapters of the agreement (on services and investment, for instance) can be subject to limitation based on the necessity to "secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to . . . the protection of the privacy of individuals in relation to the processing and dissemination of personal data". Finally, the CETA agreement, unlike the US model, does not contain a general free data flow provision and only promotes specific forms of data transfer, consistent with European economic interests, such as financial transfers for data processing in the course of business.[131]

The current European strategy regarding trade and data protection appears more clearly in the negotiations after the adoption of the GDPR. In 2018, the European Commission made public proposals on horizontal provisions for cross-border data flows, and for personal data protection in EU trade and investment agreements.[132] This template is an attempt to reconcile diverging regulatory goals, in particular human rights considerations and economic considerations.[133] This conciliation is also symbolized by the internal conflict, inside the Commission, between the

[126] EU-Korea FTA, Article 7.50 (e) (ii), OJ L 127, 14.5.2011, 1–1426.

[127] At the time, data protection was regulated under the 1995 Data Protection Directive; note 33 above.

[128] Only the investment chapter of the CETA was renegotiated after 2014. The agreement has been provisionally in force since September 2017.

[129] CETA, Article 16.3. However, Article 16.3 clarifies the possibility to submit electronic commerce to internal taxes.

[130] CETA, Article 16.4. Both the 2005 APEC and 2013 OECD privacy frameworks are therefore relevant to justify the parties' regulations.

[131] CETA, Article 13.15.1. However, the following paragraph immediately outlines that the parties are allowed "to maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information".

[132] "Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection", https://perma.cc/P6YB-7M9N.

[133] See Yakovleva, note 19 above.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press

Directorate General for Trade (DG Trade), traditionally in charge of trade negotiations, and the Directorate General for Justice and Consumers (DG JUST). DG Trade has shown greater sensitivity toward cross-border data flows, whereas DG JUST conceived trade law as an instrument to expand Europe's privacy protections.[134] As a result, this template supports cross-border data flows while also immediately recognizing that the protection of data and privacy is a fundamental right. Therefore, the protection of data privacy is exempted from any scrutiny.[135] This privacy safeguard uses the wording from a clause to the national security exceptions and contrasts with the necessity and proportionality tests put in place under the TPP and USMCA. Not surprisingly, this privacy carve-out was immediately criticized by tech business lobbyists in Brussels.[136]

However, the EU proposals formulated in late 2018, under the framework of the negotiation of two new FTAs with Australia and New Zealand (initiated in 2017), largely confirmed the template's approach. First, the EU's proposed texts refer to the right of the parties to regulate within their territories to achieve legitimate objectives, such as privacy and data protections.[137] These proposals also further cross-border data flows in order to facilitate trade in the digital economy and expressly prohibit a set of restrictions, among which are requirements relating to data localization for storage and processing, or the prohibition of storage or processing in the other party's territory. Moreover, the proposals protect the source code, providing that, in principle, the parties cannot require the transfer of, or access to, the source code of software owned by a natural or juridical person of the other party.[138] A review clause on the implementation of the latter provision, in order to tackle possible new prohibitions of cross-border data flows, is included. Additionally, the European proposals allow the parties to adopt and maintain safeguards they deem appropriate to ensure personal data and privacy provisions. The definition of personal data is similar to the GDPR's conception.[139] This approach is also in line with the EU's proposal, formulated within the context of the plurilateral negotiations regarding e-commerce, which took place at the WTO in April 2019.[140]

The ability of the EU to persuade its trading partners to endorse its vision on digital trade remains uncertain. In this context, the content of the Digital Chapter of

[134] See Streinz, note 98 above, at 334–335.
[135] See Article B.2 of the European Template.
[136] This includes "Digital Europe", which represents the largest European, but also non-European, tech companies (such as Google, Microsoft, Amazon and Huawei). See "DIGITALEUROPE Comments on the European Commission's Draft Provisions for Cross-Border Data Flows" (DIGITALEUROPE, 3 May 2018), https://perma.cc/RPB6-XGUM.
[137] Article 2 of the proposals.
[138] Article 11 of the proposals. However, this provision is potentially subject to the general exception clause of the agreement.
[139] Articles 5 and 6 of the proposals. Under Article 6.4 "personal data means any information relating to an identified or identifiable natural person".
[140] EU proposal for WTO disciplines and commitments related to e-commerce, INF/ECOM/22, 26 April 2019.

the recently concluded FTA between the EU and Japan is not very different from the CETA,[141] demonstrating the absence of real common ground and Japanese support on this issue. Whereas the JEFTA is an ambitious text in a wide range of sensitive trade matters (such as geographical indications, service liberalization and the link between trade and the environment), it only refers to a vague review clause regarding digital trade and free data flows.[142] However, as mentioned earlier, the question of cross-border data flows between Japan and the EU has been dealt with through the formal process that led Japan to reform its legal framework on data protection, which in turn led to the Commission's 2019 adequacy decision.[143] Unilateral instruments remain, for the EU, the de facto most efficient tools when it comes to the promotion of its conception of data protection.[144]

V CONCLUSION

The entry into force of the GDPR coincides with a new era of international trade tensions, which might be interpreted as a new symbol of the European "New, New Sovereigntism" envisioned by Mark Pollack.[145] The European way of addressing the issue of data processing and AI is, in reality, illustrative of the limits of the current European integration process. European industrial policies in this field have been fragmented among the member states, which have not achieved the promise of a single digital market and, even more problematically, have not faced strong international competition. So far, the EU's response to this challenge has been mostly legal and defensive in nature. Yet, such a strategy is not in itself sufficient to address the challenges raised by AI. Smart protectionism might be a temporary way for Europe to catch up with the United States and China, but any legal shield will in itself prove useless without a real industrial policy that necessitates not only an efficient regulatory environment but also public investment and, more broadly, public support. The post-COVID-19 European reaction and the capacity of the EU and its member states to coordinate their capacities, modeled on what has been done in other sectors such as the aeronautic industry, will be crucial. After all, the basis of the European project is solidarity and the development of mutual capacity in

[141] See JEFTA, Article 8.63 (promoting data transfers in the field of financial services) and JEFTA Article 8.78.3 (recognizing the importance of personal data protection for electronic commerce users).

[142] JEFTA, Article 8.81. Similarly, the new digital trade chapter of the renovated EU-Mexico FTA is limited to a three-year review clause when it comes to cross-border data flows. See EU-Mexico renovated FTA Article XX (a provisional version of the text was made public in May 2020 and is available at https://perma.cc/7TAZ-J8F9).

[143] See the Commission's Implementing Decision (EU) 2019/419 of 23 January 2019 on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, 1–58.

[144] This unilateralism does not preclude political dialogue with the partner.

[145] MA Pollack, "The New, New Sovereigntism (Or, How the Europe Union Became Disenchanted with International Law and Defiantly Protective of Its Domestic Legal Order)", in C Giorgetti and G Verdirame (eds), *Concepts of International Law in Europe and the United States* (forthcoming).

strategic economic areas, such as coal and steel in the 1950s, and a context of crisis and the risk of a decline of the "old continent" may serve as a strong catalyst for an efficient European AI policy.

On a more global and general level, the analysis of the GDPR and the European trade position on data flows and AI illustrates that this new and disruptive sector has not escaped the existing tensions between free trade and protectionism. Unsurprisingly, the new digital trade diplomacy is subject to an old rule: negotiators' positions are largely influenced by economic realities and the necessity to promote a competitive industry or to protect an emerging sector, respectively. Fundamental rights protection considerations that led to a form of "data protectionism" in the EU are certainly also influenced by its economic agenda. On the other hand, the US promotion of free flows of data essentially responds to the interest of its hegemonic companies and their leadership on the Internet and AI. The admission of the free data flows principle from the EU might correspond to the growing presence of data centers in the EU's territory, which followed the entry into force of the GDPR, given the necessity to comply with this regulation.[146] It can also be interpreted as a hand up to its trade partner, in exchange for the admission of a large data privacy carve-out that would legally secure the GDPR under international trade law. However, unless extremely hypothetical political changes occur and a willingness to forge a transatlantic resolution or a multilateral agreement on these questions materializes, the fragmentation of the digital rules on data transfer will likely remain a long-term reality.

[146] See Mishra, note 19 above, at 477.

https://doi.org/10.1017/9781108954006.011 Published online by Cambridge University Press