EXTERNAL DIMENSIONS OF EU DATA PROTECTION LAW: THE LEGAL AND THE POLITICAL

*Alessandro Petti**

Abstract

The external dimensions of EU data protection law are manifold. The provisions of EU data protection law envisage a scope of application that goes beyond the territory of the Union. Moreover, EU data transfer rules govern the mechanisms by which data could be transferred to foreign jurisdictions. In addition to this, EU law influences the development of international law in data privacy through the amendment of relevant Council of Europe Conventions and the conclusion of trade agreements. This article addresses these different external aspects of EU data protection with a focus on the relationship between law and politics. It unravels the extent to which the status of data privacy as a fundamental right in the Union comes to terms and often collides with different legal-political preferences and realities in foreign jurisdictions. It finally considers the recent initiatives of data localisation to protect EU data subject rights.

Table of Contents

1. Introduction

The reach of EU law beyond the Union's borders is a distinctive characteristic of the EU's posture as an international

legal actor. Article 3(5) TEU bestows upon the Union a constitutional mandate to uphold and promote its values and interests and contribute to the protection of its citizens in the wider world.[1] In the EU's proximity, pursuant to Article 8 TEU, such a mandate could be construed as a legal commitment on the part of the EU to shape its neighbourhood according to its values and interests.[2] The foregoing constitutional mandates have universalist drives as they are predicated on the assumption of the exportability of the EU model in the wider world. Yet, these assumptions are increasingly under strain in the current times of geopolitical fragmentation where the universality and the exportability of the EU model are put in question.

In the external dimension of EU data protection law,[3] two interrelated dynamics are at play. On the one hand, the EU overtly aspires at becoming a world leader in data protection law, possibly shaping global regulatory convergence towards its General Data Protection Regulation (GDPR).[4] On the other hand, and more importantly, the external dimension of EU data protection law serves to operate a EU-wide re-bordering outside the EU's borders. It aims at extending globally what has been powerfully described as a 'domestic utopia', that is 'a space allowing European data subjects to be at home everywhere and their personal data to flow in such a regulated and protected way that it avoids any disruption'.[5]

The article examines these joint dynamics by addressing several dimensions of the outer reach of the EU data protection law in the interplay of law and diplomacy. It brings to the fore different

* Research Fellow, Centre for European Law, University of Oslo.

[1] See also Article 21 TEU. On the reach of EU law beyond the EU's borders see M. Cremona and J. Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019).

[2] C. Hillion, *The Neighbourhood Competence under Article 8* TEU, Notre Europe Policy Paper, 2013; A. Petti, *EU Neighbourhood Law: Wider Europe and the Extended EU's Legal Space* (2024).

[3] C. Kuner, *Internet and the Global Reach of EU Law*, in M. Cremona and J. Scott, cit at 1.

[4] European Commission, 'Stronger Protection, New Opportunities -Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018', COM(2018) 43 final, 5. On these issues see also A. Bradford, *The Brussels Effect : How the European Union Rules the World* (2020).

[5] Editorial Comments, *Europe Is Trembling. Looking for a Safe Place in EU Law*, 57 Common Mkt. L. Rev 1675 (2020) 1681.

ways in which the GDPR and its antecedent directive influences foreign jurisdictions and international law. First, the article discusses the provisions of the territorial scope of the GDPR. The emphasis is placed on the interpretation of these provisions by the CJEU in its landmark de-referencing rulings (section 2). Then, the article examines the GDPR rules governing data transfer to third countries. It focusses on adequacy schemes, whereby the EU recognises that a foreign jurisdiction ensures a comparable level of protection of personal data to the EU (section 3). In that regard, the Article examines the arrangements with the US (section 3.1) and with Japan (section 3.2), with a view to appreciating the variety in the EU's engagement with foreign jurisdictions. After that, the article considers how EU law interacts with international law in the domain of data protection. After an examination of the European Economic Area (EEA) and EU-UK international law arrangements (section 4), the Article addresses the EU's involvement in the Globalisation of the Council of Europe Convention 108 (section 4.1) and discusses the interactions and frictions between the GDPR and trade regimes. Finally, the Article draws some conclusions on the dynamics of the outer reach of EU data protection law. A reflection is offered on the recent outlooks of data localisation in the EU to respond to geopolitical fragmentation.

2. The territorial scope of EU data protection law: the de-referencing rulings

The global reach of EU data protection law and the ensuing broad territorial scope of application is grounded in the EU Treaty framework. In EU law, the protection of personal data is a fundamental right enshrined in Article 8 of the EUCFR. The right to the protection of personal data is also enshrined in Article 16 of the TFEU which entrusts the European Parliament and the Council to adopt rules in the data privacy domain. The General Data Protection Regulation was adopted pursuant to both Article 8 ECFR and Article 16 TFEU.[6] Compared to the antecedent Directive

[6] 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 [2016] O.J, L 119/1.

95/46/EC,[7] the GDPR features a stronger focus on the wider reach of its application. The provisions of the GDPR, and especially Article 3, make it clear that the scope of EU data protection law goes beyond the EU territory for the processing activities of data subjects who are in the Union, even when the controller or the processor is not established within the EU.

The application of EU data protection law beyond the EU borders has been clarified in several CJEU's rulings. De-referencing rights, widely known as the 'the right to be forgotten', have inspired a landmark line of CJEU's pronouncements defining the scope of application of EU data protection law. In *Google Spain*,[8] the Court fostered an extensive interpretation of the scope of application of the EU data protection law and of the territoriality test required by Article 4(1)a of the Directive. The case concerned an EU data subject who asked Google Inc and Google Spain to remove the personal data relating to him. Entering his name on the search engine would provide links to a newspaper article where he had appeared for a real estate auction concerning repayments of social security debts.

The Court held the activities of the operator (Google Inc.) and those of the establishment situated in the Member State (Google Spain) were 'inextricably linked' because advertisement in Spain rendered the engine profitable and the engine itself constituted the means for the performance of this activity.[9] The ECJ highlighted that the display of personal data, which constitutes processing of such data, was accompanied by the display of advertising which was linked to the search term. In the words of the Court's, it was 'clear that the processing of personal data in question was carried out in the context of commercial advertising activity of the controller's establishment' on the territory of Spain.[10] The Court highlighted how the 'particularly broad territorial scope' of the Directive was designed by the EU legislature to 'prevent individuals from being deprived of the protection guaranteed by the directive'.[11] If the 'processing of personal data carried out for the purposes of the operation of the search engine [were to] escape

[7] 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, [1995] O.J. L 281/31.
[8] Case C-131/12, *Google Spain vs AEPD* ECLI:EU:C:2014:317.
[9] Ibid. para 56.
[10] ibid para 57.
[11] ibid para 54.

the obligations and guarantees' envisaged by the Directive, the 'effective and complete protection of the fundamental rights and freedoms' of EU data subjects would be compromised.[12]

What has been called the CJEU's 'limited territoriality'[13] approach in the domain of EU data protection law, has been arguably further fostered in the *Weltimmo*[14] and *Amazon*[15] cases. Although concerning intra-EU disputes, in these rulings the Court clarified the interpretation of Article 4(1)a of the Directive with arguments that could be easily applied to third-countries contexts.[16] The extensive reading of Article 4(1)a of the Data Protection Directive has led to a situation whereby its application requires a rather shallow territorial trigger, namely 'a somewhat tangible physical establishment on EU territory whose supporting activity shows at least a tiny (online) link to the actual processing activity of the third country processor'.[17] The foregoing rulings have informed the design of Article 3 GDPR. In *Google Spain,* the Court put forward an understanding whereby the wider territorial application of EU data protection law is predicated upon an interpretation informed by elements of teleological and an *effet utile* nature. [18]

In *Google v CNIL*,[19] the Court was more prudent regarding the effects of data protection law outside the Union. The case concerned a litigation initiated by Google against the French Data Protection Authority, the CNIL,[20] to contest a fine imposed by CNIL on Google Inc. for its failure to apply de-listing worldwide. Google's refusal to comply with the French Authority's formal notice imposed a penalty of one hundred thousand euros. Subsequently, Google lodged an application with the *Conseil d'État*

[12] ibid para 58.
[13] M. Gömann, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, 54 Common Mkt. L. Rev 567 (2017).
[14] Case C-230/14, *Weltimmo vs Nemzeti* ECLI:EU:C:2015:639.
[15] Case C-191/15, *Verein für Konsumenteninformation vs Amazon* ECLI:EU:C:2016:612.
[16] C. Kuner, *Internet and the Global Reach of EU Law*, cit. at 3.
[17] M. Gömann, *The New Territorial Scope of EU Data Protection Law*, cit. at 17, 574.
[18] See along the same lines S. Francq, *The External Dimension of Rome I and Rome II: Neutrality or Schizophrenia* in M. Cremona and H.W. Micklitz, *Private Law in the External Relations of the EU* (2016), 97–8. She posits: '[t]he (territorial) scope of application of EU secondary law stems from its policy objectives: a direct correlation can be established between the achievement of EU policies and the potential need to cover situations partly located in third states'.
[19] Case C-507/17, *Google vs CNIL* ECLI:EU:C:2019:772.
[20] CNIL stands for : *Commission nationale de l'informatique et des libertés*.

contesting the adjudication that resulted in the imposition of the fine. The French Court's preliminary reference revolved around the territorial scope of the Directive 95/46 and of the de-referencing rights on the basis of its provisions enshrined in its Articles 12(b) and Article 14(1)a. The ECJ adjudicated the case by not only interpreting the Directive but also the GDPR, which in its Article 17, governs the 'right to erasure'.[21]

In *Google v CNIL,* the Grand Chamber had to reconcile different approaches and rationales with respect to the outer reach of EU data protection law. A first teleological rationale,[22] predicated upon the objectives of the EU data protection law,[23] led the Court to find an EU competence and justification for a global de-referencing on all the versions of an operator's search engine.[24] While this first rationale would suggest a wider interpretation of the reach of EU data protection law, other considerations pertaining to the legal and political realities outside the EU suggested circumscribing of the application of EU data protection law. In this respect, the ECJ clarifies that the 'right to the protection of personal data is not an absolute right' and should be balanced against other fundamental rights in accordance with the proportionality principle'.[25] For instance, while benchmarks and organisational mechanisms allow for the balancing of public interest and data protection within the EU,[26] outside the Union these mechanisms may not be present.[27] In *Google v CNIL*, thus the Court found that when the search engine operator grants a delisting request in pursuance of EU data protection law, the operator 'is not required to carry out that de-referencing in all versions of the search engine, but on the version of that search engine corresponding to all the Member States'. This would be sufficient also in light of the

[21] *Google vs CNIL*, cit. at 19, para 46.
[22] Ibid, paras 54–55
[23] Especially those apparent from recital 10 of the Directive 95/46, cit at 7, and recitals 10,11, and 13 of the GDPR, cit. at 6.
[24] *Google vs CNIL*, cit. at 19, paras 57–58.
[25] Ibid, para 60.
[26] Case C-136/17, *GC and Others v CNIL,* ECLI:EU:C:2019:773, para 59. New developments in the balancing between the right to privacy enshrined in Articles 7 and 8 of the EUCFR and the right to information pursuant to Article 11 EUCFR, within the Union has come from the Grand Chamber Ruling in Case C-460/20 *TU, RE v Google LLC*, ECLI:EU:C:2022:962 regarding the obligation of de-referencing with regard to inaccurate information.
[27] *Google vs CNIL*, cit. at 19, paras 61-63

techniques of 'geo-blocking' that prevent or at least discourage users from accessing the links for which the de-referencing request has been submitted.[28]

Political motives lie behind the limitation of the territorial scope of EU data protection law. While evoked by the Advocate General, such motives were not explicitly mentioned by the Court. In fact, Advocate General (AG) Szpunar alluded to the political risks that global de-referencing orders issued by EU law would have on the possibility for individuals in third countries to have access to information. Moreover, the AG signalled that this would make third countries' regimes liable to become part of a 'race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale'.[29] Arguably, the Court's favour towards a restriction of de-referencing in the EU seems also to respond to the need to prevent international frictions with the US system. Here, the constitutional architecture grants special protection to the right to free speech, as provided for in the First Amendment to the US Constitution.[30]

The Court's approach has left EU data protection law with a fundamental ambivalence. If on the one hand, the Court established the existence of the EU competence to impose de-referencing to all the versions of a search engine to meet EU law data protection objectives, on the other hand, it subjects the exercise and the calibration of this competence to considerations of an ultimate political nature[31] pertaining to the conduct of international relations. Such a fluctuation can be also found in the text of the judgment which reads that 'while […] EU law does not currently require that the de-referencing granted concern all versions of the search engine […] it does not prohibit such a practice'. It is therefore left to the national data protection authorities to balance data privacy with the freedom of information with the possibility 'to order, where appropriate, the operator of that search engine to

[28] ibid 65; 73.

[29] Opinion of AG Szpunar, Case C-507/17, *Google vs CNIL* ECLI:EU:C:2019:15, para 61.

[30] J. Globocnik, *The Right to Be Forgotten Is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)*, 69 GRUR International 380 (2020), 386.

[31] Editorial Comments, *Europe Is Trembling. Looking for a Safe Place in EU Law*, cit. at 5 1680.

carry out a de-referencing concerning all the versions of that search engine'.[32]

The foregoing calibration is not an isolated approach in the realm of EU internet law. A similar attitude has been endorsed in the case of the e-Commerce Directive[33] whereby the Court established that the design of the directive and the injunction measures to be taken by national courts pursuant to Articles 15 and 18 of the Directive, do 'not preclude those injunction measures to have effects worldwide'. The Court found that it is 'up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account' of rules applicable at the international level.[34] In *Glawischnig-Piesczek v Facebook*, the Court established that Article 15 (1) of the E-commerce Directive 'must be interpreted as meaning that it does not preclude a court of a Member State from […] ordering the host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law'.[35]

Some days before the delivery of the *Google v CNIL* pronouncement by the Grand Chamber, the Third Chamber of the ECJ had arguably taken a different stance in *Glawischnig-Piesczek v Facebook*. In this case the Court's decision actually established the worldwide deletion of unlawful content. Yet, its reasoning was similar to the one of *Google v CNIL*. While recognising also in this case the competence derived from EU law to order the worldwide deletion, the ECJ left the national courts with a margin for manoeuvre to order the deletion of unlawful content pursuant to Article 15(1) of the Directive.[36] This line of reasoning also suggests that EU data protection law may be applied globally along the lines of what the Court found in *Google Spain*.

In *Google Spain*, the Court had linked the scope of application of the Data Protection Directive to a primarily teleological interpretation of EU law. In *Google v CNIL*, the Court qualified the perimeter of the *effet utile* of EU law calibrating the teleological approach adopted in *Google Spain* with a proportionality-based

[32] *Google vs CNIL*, cit. at 19, para 62.
[33] Directive 95/46/EC cit. at 7.
[34] Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821, paras 51–52.
[35] ibid 53.
[36] J. Globocnik, *The Right to Be Forgotten Is Taking Shape*, cit. at 3o, 387 fn 82.

assessment. This responds to the design of Article 52 EU Charter of Fundamental Rights (EUCFR). Indeed, although not explicitly mentioned, in *Google v CNIL*, the approach taken by the Court suggests a limitation of the exercise of the rights and principles of EU law as provided for in Article 52 (1) of the EUCFR.[37] The Charter envisages limitations to the rights it safeguards insofar as 'they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. Crucially, the Court limited the territorial scope of de-referencing rights of EU data by simultaneously mandating a broader territorial application to the limitations envisaged by Article 52 (1) of the EUCFR. This ambivalence found a composition in the principled and pragmatic attitude of the Grand Chamber in *Google CNIL*. On the one hand, the Court intimates that de-referencing can possibly be applied globally as this would be within the competences granted by EU law. On the other hand, it recognises that an EU-wide de-referencing combined with geo-blocking is sufficient to safeguard the *effet utile* of EU law while adapting it to different political contexts.

3. The law and politics of data transfer: the adequacy decisions

The external dimension of the GDPR is not limited to its territorial scope ranging outside the EU in pursuance to the provisions of its Article 3. A crucial aspect of the cross-border data protection of the GDPR pertains to the data transfer rules detailed in chapter V of the Regulation. In that regard, the tripartite structure allowing for data transfer outside the Union (adequacy, appropriate safeguards, exceptions) envisaged by the antecedent Directive has been broadly replicated in the Regulation.[38] First, data transfer from the EU to third countries is allowed in the case of an adequacy decision. In those decisions, the Commission recognises that the country at issue offers an adequate level of protection of EU data privacy, comparable to that accorded by EU law. Adequacy decisions may be construed as entailing an extension of the EU's

[37] This was instead rendered explicit in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (*Schrems II*) ECLI:EU:C:2020:559.

[38] See further C. Kuner, *Internet and the Global Reach of EU Law*, cit. at 3.

legal space as they trigger convergence to EU law. In making the adequacy assessment, the Commission considers factors such as the rule of law and respect for human rights and fundamental freedoms (Article 45 GDPR). Secondly, data transfer is allowed subject to appropriate safeguards provided by the data controller or the data processor (Article 46) such as Standard Data Protection Clauses (SDPC) and Binding Corporate Rules (BCRs) recognised by Member States' competent supervisory authorities (Article 47). An additional venue for data transfer consists in specific derogations such as consent by the data transfer, performance of a contract, or reasons of public interest (Article 49).

Data transfer rules are crucial in understanding the relationship between the EU with foreign jurisdictions and the interplay of law and diplomacy. The data transfer rules of the GDPR display more evidently diplomatic elements: they often entail a differentiation in the relationship with third countries that is typical of international relations. The factors that the Commission needs to consider when issuing the adequacy decision are detailed in Article 45 GDPR. Arguably adequacy decisions are a synthesis of different ways in which EU data protection law influences and interacts with foreign jurisdictions.

In the mechanisms highlighted by Kuner whereby EU data protection law influences foreign jurisdictions, adequacy decisions mainly pertain to 'coercion and conditionality'.[39] While there is not a veritable coercion, conditionality is at play in so far abidance by EU (or equivalent) standards is rewarded with EU market access. Political elements are usually factored in the framework of adequacy talks. While the Commission maintains for instance that 'EU data protection rules cannot be the subject of negotiations in a free trade agreement',[40] it recognises that although 'the protection of personal data is non-negotiable, [..] the EU regime on international data transfers […] provides a broad and varied toolkit to enable data flows in different situations'.[41] Especially in the past, there have been instances where adequacy determinations became 'entangled in political issues', also engendering frictions with third countries deemed to have not been treated equally in the

[39] Ibid.
[40] European Commission, 'Exchanging Personal Data in a Globalised World' COM(2017) 7 final, 9.
[41] ibid 6.

assessment of their legal systems.[42] For instance, the EU adequacy determination in Argentina has been described as amounting to a 'reward for adopting an EU-style data protection law at a time when such legislation had not yet spread throughout Latin America, let alone the world'.[43]

EU data transfer rules largely follow a geographic approach. As noted by Kuner, such an approach is predicated upon the jurisdiction to which the data are to be transferred. In that context, adequacy decisions serve to determine whether the foreign jurisdiction importing data ensure adequate standards of protection both in the design and the implementation of the relevant data protection law. This stands in contrast to an organisational approach whereby the 'data exporters [are made] accountable for ensuring the continued protection of personal data transferred to other organizations no matter what their geographic location'.[44] The following sections will illustrate how the geographic approach of adequacy decisions is hardly monolithic. There are different articulations of adequacy frameworks in different jurisdictions.

3.1 EU data protection in the US

Three frameworks for data transfer have been negotiated between the EU and the US. Two have been invalidated by the EU Courts, a third is currently under scrutiny by the CJEU. The *Safe Harbour* was a first arrangement allowed the transfer and processing of data on the basis of a set of voluntary principles and practices upheld by US companies adhering to it. The delicacy of the negotiations principally arose from the different EU and US approaches to the matter. While the US's preferences 'remained

[42] C. Kuner, *Transborder Data Flows and Data Privacy Law* (2013) He writes: 'in July 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports. In addition, members of the Article 29 Working Party have told the author that politics entered into that group's decision to approve Argentina as providing an adequate level of data protection, and a failed bid for adequacy by Australia in the early 2000s caused tensions between that country and the EU', 66.
[43] P.M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771 (2019).
[44] C. Kuner, *Transborder Data Flows and Data Privacy Law*, cit. at 42, 64.

markedly anti-regulation',[45] EU as its Member States were 'extremely sceptical of the very notion of industry self-regulation'.[46] An additional contentious issue pertained to the effectiveness of enforcement schemes for effective protection of individuals' privacy (primarily demanded by the EU) and the formulation of a predictable legal framework (as advocated by the US). Notwithstanding some objections by the European Parliament, the Commission eventually established that the *Safe Harbour* would be in compliance with EU adequacy criteria.[47] After the invalidation of the arrangement in *Schrems I*, the EU negotiated a second arrangement the *Privacy Shield* that resulted in a second adequacy determination. This second framework mirrored the first in many respects, although the enforcement mechanisms were strengthened, and reassurances were given with respect to the fact that the data transferred under the *Privacy Shield* would not be subject to programmes of mass surveillance.[48]

In its dismissal of the *Safe Harbour* scheme, the Court maintained that '[US] legislation permitting public authorities to have access on a *generalised basis* to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.[49] Moving away from the Advocate General's suggestions, [50] the Court noticed significant flaws the principles of the *Privacy Shield* in favour of US interests and rules.

---

[45] European Commission, Press Release - Speech by Mario Monti- "The Information Society: New Risks and Opportunities for Privacy" (Brussels, 18 October 1996).

[46] D. Heisenberg, *Negotiating Privacy : The European Union, the United States, and Personal Data Protection* (2005) 87.

[47] Commission Decision (EC) 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), [2000] OJ L 215/7.

[48] US Administration, 'Letter from Robert S. Litt, General Counsel, Office of the Dir. of National Intelligence, to Justin S. Antonipillai, Counselor, U.S. Department of Commerce, and Ted Dean, Deputy Assistant Security, International Trade Administration.' (22 February 2016).

[49] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner (Schrems I)* ECLI:EU:C:2015:650, para 94 emphasis added.

[50] Opinion of AG Saugmandsgaard Øe, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2019:1145, paras 174–186.

Limitations on data protection of EU data subjects were, in fact, still envisaged when 'necessary to meet national security, public interest, or law enforcement requirements in the US'.[51] Besides, the domestic law of the US[52] was considered by the CJEU to be unsatisfactory with regards to the guarantees of proportionality in establishing limitations on the protection of personal data. The proportionality of these limitations was mandated by EU constitutional requirements enshrined in Article 52(1) of the ECFR.[53] Shortcomings were also found with respect to the lack of effective remedies pursuant to Article 47 of the Charter. In fact, the Commission itself had noticed the possible unlawful surveillance of EU data subjects for US national security purposes.[54]

In both *Schrems I* and *Schrems II* the Court attempted to insulate the negotiated adequacy framework from political interferences at both sides of the negotiating tables. The empowerment of EU national data protection authorities operated by the Court in *Schrems I* at the expenses of the Commission[55] can be read as an attempt to separate political negotiations from legal monitoring and assessment on the EU side. In adequacy decisions, in fact, the Commission both designs the negotiations of the data protection framework and monitors the adequacy. In the words of Azoulai and van der Sluis, in *Schrems I*, the Commission was 'regarded by the Court as a political body and not as a technical body responsible for the oversight of Union law'.[56] The independence of the data protection framework from political influences on the US side was a crucial motive of the *Schrems I* and *Schrems II* rulings. In *Schrems II*, the Court found the remedies to the Ombudsperson Mechanism introduced by the US authorities insufficient. The Court expressed reservations with regard to the political role of the Ombudsperson: although the Ombudsperson is considered as 'independent from the Intelligence Community', she was described as '[reporting] directly to the Secretary of State and

[51] *Schrems II* (n 43) para 164.
[52] In particular the Foreign Intelligence Surveillance Act, notwithstanding the limitations prescribed by the Presidential Privacy Directive (PPD)- 28.
[53] Case C-311/18, *Schrems II,* cit. at 37, paras 168–185.
[54] Ibid, paras 190–191.
[55] Case C-362/14, *Schrems I*, cit. at 49, paras 44–45.
[56] L. Azoulai and M. van der Sluis, *Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: Schrems*, 53 COMMON MKT. L. REV. 1343 (2016), 1359.

is an integral part of the US State Department'. Besides, the appointment and the dismissal of the Ombudsperson was not accompanied by guarantees of her independence from the executive and there was 'nothing in [the *Privacy Shield* Decision] to indicate that ombudsperson has the power to adopt decisions that are binding on [the] intelligence services'.[57]

The CJEU's endeavours to safeguard the EU's data protection standards from the interferences of the political process has constitutional significance. In the foregoing rulings, the Court has established that limitations to the scope and intensity of application of EU data protection law in the third country context is regulated by Article 52(1) of the EUCFR. The EUCFR is not intended to be territorially limited. Data transfer of EU data subjects outside the EU must thus occur within the same protection and safeguards accorded internally by the EU legal order. The assessment of the 'essential equivalence' to be carried out by the Commission when negotiating with third countries needs thus to be undertaken at the level of EU primary law.[58]

On 10 July 2023 the Commission adopted a new adequacy decision for the US. In its annexes, the decision encloses the EU-US Data Privacy Framework (DPF) issued by the US Department of Commerce. The DPF is the product of the US's last attempts to set up legal arrangements compliant with the EU data privacy rules to promote trade. As the previous decisions, the Commission's DPF-related adequacy decision is 'partial' insofar as it covers the processing of personal data only of those US organisations that voluntary decide to certify under the EU-US DPF. Arguably the timing of the EU-US adequacy framework has been influenced by geopolitical events, not least the war in Ukraine. The adequacy determination, indeed, become entangled with the political need to show a united front against Russian aggression also in the sensitive domain of internet and data privacy.[59]

The renewed EU-US Data Privacy Framework endeavours to address the main reservations put forward by the ECJ in *Schrems*

---

[57] Case C-311/18, *Schrems II,* cit. at 37, paras 194–197.

[58] S. Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities"*, 21 The Journal of World Investment & Trade 881 (2020), 913.

[59] 'US Eyes Breakthrough on Data Dispute with EU as Biden Visits Brussels' (*POLITICO*, 24 March 2022) <https://www.politico.eu/article/us-eyes-breakthrough-on-data-dispute-with-eu-biden-visit-privacy-shield-ukraine/> accessed 27 August 2024.

II which elicited an overhaul of US data privacy rules. President Biden's Executive Order (EO) 14086 better articulates the objectives to be pursued by intelligence activities with respect to the Presidential Policy Directive 28 issued by the Obama administration, whose critical points regarding EU privacy law had been highlighted by the ECJ's in *Schrems II*. Yet, the definition of some of the objectives remain nebulous and it has been noted how the EO does not modify the existing US intelligence legislation, which allows for the surveillance of non-US citizens abroad.[60] Moreover, with regard to the right to an effective remedy and fair trial as provided for in Article 47 ECFR, the European Data Protection Board casted doubts on whether the 'rules set forth in EO 14086 and its supplemental provisions, in particular those designed to foster the DPRC's independence, are fully implemented and are functioning effectively in practice'.[61] The resolution of the European Parliament has been even more critical by affirming that the EU-US Data Privacy Framework 'fails to create essential equivalence in the level of protection' of data. The attention of the European Parliament Resolution focused on the scarce independence of the DPRC in light of the appointment and revocation rules of its members. The Resolution noted how the DPRC is 'part of the executive branch and not the judiciary'. In the European Parliament view, the DPRC does not meet the standards of independence and impartiality of Article 47 of the EU Charter. [62]

It remains to be seen whether the new EU-US DPF will pass the tests of the CJEU. New episodes of the EU-US data transfer judicial saga are in the making, with cases on the validity of the EU-US adequacy framework pending before the CJEU.[63] The constitutional rigidity of the EU data protection framework does not only pertain to the US frameworks, but it can be also evinced

[60] S. Batlle and A. van Waeyenberge, *EU–US Data Privacy Framework: A First Legal Assessment*, 15 Eur. J. Risk Regul. 191 (2024), 195.

[61] European Data Protection Board, 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework', 28 February 2023, 46-47.

[62] European Parliament Resolution, Adequacy of the protection afforded by the EU-U.S. Data Privacy Framework, P9_TA(2023)0204, point 9

[63] Case T-553/23, *Latombe v Commission*, Order of the President of the General Court.

from the CJEU's invalidation of the Passenger Name Record (PNR) agreement negotiated with Canada.[64]

3.2 EU data protection in Japan

The EU-Japan free trade area is an additional example of the level to which EU regulatory autonomy in data privacy is upheld to protect the EU's constitutional fabric. In 2019, the EU and Japan announced a mutual adequacy framework that was acknowledged as the world's largest area of safe data flows.[65]The Commission Communication heralding the achievement of the adequacy arrangement somewhat recognised the underlying asymmetry of the framework. In fact, it was for Japan to introduce 'additional safeguards to guarantee that data transferred from the EU [would] enjoy protection guarantees in line with European standards'.[66] The process of alignment of Japanese law to EU standards resulted in amendments to the Japanese Act on the Protection of Personal Information (APPI) and the Personal Information Protection Commission (PPC). These instruments and bodies were modelled along the lines of the EU national data protection authorities.[67] It should be noted how the adequacy scheme pertains only the private sector. At the time of the granting of the adequacy decision, the public sector, including the law enforcement and the national security agencies, was governed by a separate regime, which does not envisage the supervision of the PPC.[68]

The adequacy arrangement with Japan rests upon the Supplementary Rules featured in the Annex of the Adequacy

---

[64] Opinion 1/15, *PNR EU-Canada* ECLI:EU:C:2017:592.

[65] European Commission, Press Release, 'European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows' (*European Commission*)<https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421>.

[66] ibid.

[67] Y. Miadsvetskaya, *What Are the Pros and Cons of the Adequacy Decision on Japan?* CITIP *blog -KU Leuven, Law* 2019, <https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/>.

[68] H. Miyashita, *The EU-Japan Relationship*, *blogdroiteuropéen* (2020), 4 <https://blogdroiteuropeen.com/wp-content/uploads/2020/06/miyashita-redo.pdf>.

determination.[69] These 'Supplementary Rules', under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU, were adopted by the Japanese PCC on the basis of Article 6 of the Act on the Protection of Personal Information. Supplementary Rules implement additional requirements on the processing and transfer of the data of EU data subjects. In the words of the Commission, they 'were put in place to bridge certain relevant differences between the APPI and the GDPR'.[70] The requirements at issue are more stringent than those envisaged by Japanese legislation for Japanese data subjects.[71] For instance, supplementary Rules 'ensure that data subject rights will apply to all personal data transferred from the EU, irrespective of their retention period'.[72] Instead, domestically, the Japanese legal system envisages that data subject rights do not apply to personal data which are intended to be deleted within a period of six months.[73] Moreover, the PPC agreed to broaden the scope of the categories of sensitive data to also include sexual orientation.[74] In light of the foregoing, the different regimes could thus lead to discrimination between EU and non-EU data subjects within the Japanese jurisdiction.[75]

Different philosophies underlie data protection rules in the EU and Japan. While in the Union data protection law is primarily informed by fundamental rights rationales, in Japan it is predicated upon WTO requirements.[76]As a matter of fact, the Japanese data protection system remains primarily premised upon business interests more than on a rights-based attitude.[77] The adequacy

[69] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation EU 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76/1. See text to fn 79 of this article for the developments in the public sector.

[70] European Commission, 'Report on the first review of the functioning of the adequacy decision for Japan', COM(2023) 275 final, 1.

[71] See Commission Implementing Decision (EU) 2019/419, cit. at 69, Annex I.

[72] European Data Protection Board, 'Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan', adopted on 5 December 2018, 5.

[73] ibid.

[74] ibid.

[75] H. Miyashita, *The EU-Japan Relationship*, cit. at 68, 5.

[76] ibid 13.

[77] F. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 Harv. J.L. & Tech. (2020), 688.

determination in Japan has been recently confirmed by the EU.[78] A welcomed development has been the transformation of the 'APPI into a comprehensive data protection framework covering both the private and public sector, subject to the exclusive supervision of the PPC'.[79]This could extend the scope of the EU-Japan adequacy framework to cover also the areas of regulatory cooperation and research. With regard to enforcement, it has been questioned whether Supplementary Rules are enforceable by the Japanese Courts.[80] At the times of the review of the EU-Japan adequacy decision, the PPC reported that it had received no complaints concerning compliance with the Supplementary Rules and that it was considering, on its own initiative, random checks to ensure compliance, an announcement welcomed by the Commission.[81]

4.The GDPR and the interface between EU law and international law

The interface between EU law and international law is key in understanding the protection and projection of EU data rules between the EU's borders. The EU has a constitutional mandate to uphold its values and interests in the wider world.[82] This mandate is arguably stronger in the EU's proximity[83] and pertains also the diffusion of the EU data protection model. A key arrangement for the extension of EU law in the Union's proximity is the European Economic Area Agreement. The Agreement aims at a 'continuous and balanced strengthening of trade and economic relations between the Contracting Parties' on the basis of 'the respect of the same rules'.[84] In force between the EU and its Member States on the one hand, and Norway, Iceland and Liechtenstein on the other hand, the EEA Agreement is a dynamic association agreement that

[78] European Commission, 'Report on the first review of the functioning of the adequacy decision for Japan', COM(2023) 275 final, 6.
[79] Ibid. 4.
[80] H. Miyashita, *The EU-Japan Relationship*, cit. at 68, 6.
[81] European Commission, 'Report', cit. at 78, 5.
[82] See Articles 3(5), 21 TEU.
[83] Article 8 TEU. See also A. Petti, *EU Neighbourhood Law*, cit. at 2.
[84] Article 1 European Economic Area Agreement, [1994] OJ L1/3.

evolves with the substantive evolution of EU secondary law.[85] The GDPR has been incorporated in the EEA Agreement through a Decision of the Agreement's Joint Committee.[86] In pursuance to the principle of homogeneity,[87] in both in the EU and in the EEA-EFTA pillar of the EEA data subjects and undertaking will have the same rights and obligations. Yet, the constitutional setup of the EEA Agreement is different from the one of the EU. The EU Treaties have a status of a constitutional charter.[88] The EEA, instead, has been characterised by the ECJ as an international treaty 'which essentially, merely creates rights and obligations as between Contracting Parties and provides for no transfer of sovereign rights to the inter-governmental institutions which it sets up'. [89]A key difference in terms of primary law between the EU and the EEA-EFTA pillar rests on the fact that the EUCFR is not part of the EEA Agreement. While the legal effects of the GDPR are the same in the EU and EEA EFTA-pillar, the sources of law are different. This is reflected in the preamble of the GDPR and the corresponding legal act incorporated into the EEA Agreement. The GDPR makes several references to the GDPR both in the preamble as it regards the legal basis and in the body of the Regulation. However, while the adapted EEA act recognises the fundamental rights nature of data protection, it does not evince this from the EU Charter but from 'various international human rights agreements'.[90] The references to the EU Charter are deleted from the text.[91]

Remaining in the EU's proximity, the new EU-UK relations are governed by the Trade and Cooperation Agreement (TCA), which is an Association Agreement like the EEA Agreement. It should be noted, however, that the purposes and the scope of the EEA Agreement are different from those of the EU-UK TCA. Only the former is predicated upon the extension of EU law to the EEA

[85] M. Cremona, *The "Dynamic and Homogenous" EEA: Byzantine Structures and Variable Geometry*, 19 Eur. L. Rev. (1994) 508.
[86] European Economic Area, Joint Committee Decision No 154/2018, [2018] OJ L 183/23.
[87] See *inter alia*, Article 1 and Chapter 3 EEA Agreement, cit. at 84.
[88] Case 294/83, *Les Verts*, EU:C:1986:166, para 23
[89] Opinion 1/91, *EEA Agreement*, ECLI:EU:C:1991:490.
[90] Recital 2, European Economic Area, Joint Committee Decision No 154/2018, cit. at 86.
[91] Ibid, Article 1(i) with regard to Article 58(4) GDPR.

EFTA states.[92]The EU-UK TCA is based on international law and does not envisage the extension of EU rules.[93]The data transfer between the EU and the UK is currently based on an adequacy decision granted by the Commission in 2021.[94] In its assessment of the UK legal framework, the Commission grounded its decision on the fact that GDPR forms in its entirety part of 'retained EU law'.[95] As the Commission highlights on the basis of the UK legislation, unmodified retained EU law must be interpreted in accordance with the CJEU case law and the general principles of EU law.[96] The general framework of the EU-UK association pursuant to the TCA remains crucial, as this is based on the continuous protection of human rights and fundamental freedoms, including the protection of personal data.[97] The Commission will thus continuously monitor the application of the UK legal developments in the adequacy framework.[98] As recently pointed out by the ECJ's Grand Chamber, the withdrawal of the UK from the EU has dispelled the presumption of mutual trust which is proper to EU membership and extended through the special legal relationships between the EU and the EEA EFTA states.[99]This makes the continuous monitoring even more necessary.

4.1 The globalisation of CoE Convention 108

The use of international law to indirectly promote convergence to EU law is one of the mechanisms through which the EU influences foreign jurisdiction and promotes the development of international law. This is not a novelty in EU external relations law, and it emerges here in the relationship between the GDPR and

[92] See in this respect the seminal findings of the CJEU in Case T- 115/94, ECLI:EU:T:1997:3.
[93] For a problematisation see A. Petti, *EU Neighbourhood Law*, cit. at 2, chapter 7.
[94] European Commission, Implementing Regulation 2021/1772, [2021] OJ L360/1.
[95] UK, European Union Withdrawal Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/contents
[96] European Commission, Implementing Regulation 2021/1772, cit. at 94, point 13.
[97] This is especially the case of Part III of the TCA on Law Enforcement and Judicial Cooperation in criminal matters, particularly Articles 524, 525, 692 EU-UK Trade and Cooperation Agreement [2021] OJ L 149/10.
[98] Article 3 European Commission, Implementing Regulation 2021/1772, cit. at 94, point 13.
[99] See Case C-202/24 [*Alchaster*], EU:C:2024:649.

Convention 108 of the Council of Europe and its additional Protocol. First, the adoption of Convention 108 of the CoE by third countries serves as a prerequisite for obtaining EU adequacy decisions.[100] Convergence to EU law is then mediated by international law instruments. Secondly, via the participation of its Member States in the Convention, the EU contributes to the substantive development of international law instruments in accordance with EU law and the Union's policy preferences. Clearly, the ensuing dual process is beneficial for the EU as it amounts to a promotion of its interests, and the safeguarding of its citizens' rights.

The EU's influence over the 108 CoE Convention illustrates how the EU masters international negotiations to extend the reach of its law and its standards. As early as 2001, the Convention was amended with the adoption of its Additional Protocol that brought the Convention closer to the Directive 95/46/EC then in force.[101] The Protocol introduced the obligation to appoint a data protection authority and the mandatory requirement of restrictions for data export. The Convention thus borrowed EU law's paradigms of export restriction. Further attempts to bridge the gap between EU law and Convention 108 have been undertaken in the process of the 'modernisation' of the Convention which ran in parallel to the design of the GDPR. The relevant negotiations were concluded on 18 May 2018, a few days before the GDPR entered into force. On the substantive level, the 'Modernised Convention' (Convention 108+)[102] incorporates the fundamental principles of the GDPR including additional restrictions on some sensitive processing systems (Art. 8bis (2)), limitations on automatic decision-making, and the right to object to processing on legitimate grounds (Article 8(a-c)).[103]

---

[100] See Recital 105 and Article 45(2)c of the GDPR and European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' cit. at 40, 11.

[101] G. Greenleaf, *A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108*, in D. Lindsay and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (2014) 96.

[102] Council of Europe, 'Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data', adopted by the of Ministers at its 128th Session of the Committee of Ministers, Elsinore, 18 May 2018.

[103] G.Greenleaf, *Renewing Convention 108: The CoE's "GDPR Lite" Initiatives* (Social Science Research Network 2016) SSRN Scholarly Paper ID 2892947 3 <https://papers.ssrn.com/abstract=2892947>.

The Convention's process of modernisation was intertwined with the initiative of its membership enlargement to non-European countries. This was done utilising the latent provision of Article 23(1) of the Convention. It is worth mentioning that, the law enforcement cooperation dimension was a key driver in the EU's engagement in the globalisation of the convention. In fact, the adoption of the Convention is considered by the EU as a 'reassurance that international protection standards are met' also with a view to international cooperation with Eurojust and Europol.[104]

In the EU-UK TCA, the Article on the Protection of personal data[105] in the context of law enforcement cooperation is located immediately after that on the sources of law on the protection of human rights and fundamental freedoms that assigns a prominent role to the ECHR. The safeguarding of data protection rights features prominently in the agreement especially with respect to Part III on law enforcement and judicial cooperation in criminal matters. Here, 'in the event of serious and systemic deficiencies within one Party as regards the protection of personal data, including where those deficiencies have led to a relevant adequacy decision ceasing to apply', the other Party is entitled to suspend this part of the agreement.[106]

In its engagement in the negotiations of the Convention, the EU managed to carve out some exceptions with a view to safeguarding the autonomy of the EU legal order. In the relevant Protocol, an exception was created for groups of states, such as the EU, which could enjoy an advantageous status within the Convention regime. Regional organisations such as the EU were allowed to set higher standards to be fulfilled than those established by the Convention. As highlighted by Greenleaf: 'what previously appeared to be only "maximum" allowed standards in the old Convention has now become another "minimum" required in the new one, but only where it is a standard adopted by a group of

[104] ibid 5; L.A. Bygrave, *The "Strasbourg Effect" on Data Protection in Light of the "Brussels Effect": Logic, Mechanics and Prospects*, 40 Comput. L. & Sec. Rev. (2020).
[105] Article 525 EU-UK TCA, cit. at 97.
[106] See Article 693(2) EU-UK TCA, cit. at 97. See Also Part I. A. 7 of the EU-UK Political Declaration in 2019: 'The future relationship should incorporate the United Kingdom's continued commitment to respect the framework of the European Convention on Human Rights (ECHR)'.

parties'.[107] This may be regarded as a manifestation of EU exceptionalism in international law. In fact, EU law is insulated from the relevant international law regime with a view to safeguarding its legal autonomy. It should be noticed, however, how these mechanisms allowing for an accommodation between the EU and the CoE regime are also in themselves a driver for the globalisation of the Convention.

Thanks to the relative flexibility of the Convention, its globalisation arguably results in the globalisation of the EU model of data protection law. In this respect, Mantelero highlighted that 'it is more important to define a global standard [Convention 108+] than a golden one [GDPR]' as only the former 'can be fully effective in those countries unable to reach the golden standard'.[108] The Convention is also the sole binding international law instrument in which membership is virtually not geographically limited.[109] Indeed, other international agreements on data protection are either of a soft law nature (OECD Guidelines and Asia-Pacific Economic Cooperation (APEC) framework) or contemplate only regional membership (EU GDPR or the supplementary Act on Personal Data Protection within the ECOWAAS).[110]

It is worth noticing how adherence to the Convention standards is seen as conducive to facilitating the adequacy process. For instance, Morocco was among the first non-CoE countries to join the 108 Convention and its Additional Protocol.[111] Morocco's achievement was a product of CoE neighbourhood Partnership in 2018-2021. This programme, financed also by the EU, aimed at consolidating democratic changes and the respect of human rights and the rule of law.[112] Adherence to Convention 108 CoE thus is thought to play a propaedeutic role for access to the EU's legal space on data protection. In the words of the then president of the

[107] G. Greenleaf, *Renewing Convention 108: The CoE's "GDPR Lite" Initiatives*, cit. at 103, 2.
[108] A. Mantelero, *The Future of Data Protection: Gold Standard vs. Global Standard*, 40 Comput. L. & Sec. Rev. (2021), 4.
[109] S. Kwasny, A. Mantelero and S. Stalla-Bourdillon, *The Role of the Council of Europe on the 40th Anniversary of Convention 108*, Comput. L. & Sec. Rev. (2021), 1.
[110] G. Greenleaf, cit. at 101, 94–5.
[111] See section 4.1 of this Article.
[112] Council of Europe, Neighbourhood Partnership with Morocco 2018-2021, Document approved by the by the Committee of Ministers of the Council of Europe on 21 March 2018 (CM/Del/Dec(2018)1311/2.3).

Moroccan Data Protection Authority, accession was regarded as 'an important step in the [EU] adequacy process'.[113]

4.2 Trade regimes and EU data protection law

The interaction between EU data protection law and international law is not only limited to the protection of human rights but also the regulation of international trade. The EU's institutional discourse emphasises that the intersection between human rights and trade in data protection law has a twofold dimension. On the one hand, the protection of personal data is considered as a 'competitive differentiator and a selling point on the global marketplace'.[114] On the other hand, common standards with a wide territorial reach contribute to 'creating a level playing field with companies established outside the EU'.[115]

EU data protection law and particularly the GDPR affects trade in services falling within the remit of the WTO General Agreements on Trade in Services (GATS). As a matter of fact, the GDPR governs the transfer of personal data beyond the EU. It applies to cross-border transactions in services entailing the transfer of personal data of EU data subjects even in cases where the processing of data occurs outside the EU and the EEA.[116]

Yakovleva and Irion[117] identify several points of friction between EU data protection law and GATS. First, adequacy decisions issued by the Commission might be considered to be in breach of the most-favoured-nation treatment (MFN)[118] as the EU

---

[113] 'Données personnelles: Le Maroc adhère à la Convention 108' (*L'Economiste*, 11 June 2019) <https://www.leconomiste.com/article/1046086-donnees-personnelles-le-maroc-adhere-la-convention-108>.

[114] European Commission, 'Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation', COM(2020) 264 final, 3.

[115] ibid 9.

[116] S. Yakovleva and K. Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, 114 AM. J. INT'L L. 10 (2020), 10–11.

[117] Ibid.; S. Yakovleva and K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection,* 2 Eur. Data Prot. L. Rev. 191 (2016); K. Irion, S. Iakovleva and M. Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements*, (2016). Available at SSRN: <https://ssrn.com/abstract=2877166 or http://dx.doi.org/10.2139/ssrn.2877166>.

[118] GATS Article II.1 which reads: 'With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to

grants a more favourable regime of data transfer to countries that have obtained an adequacy determination.[119] Moreover, EU data protection law could potentially be found to be in breach of the national treatment obligation.[120] Indeed, provision of services and service suppliers established in countries which have not been granted an adequacy determination will have to comply with the stringent GDPR requirements. This may entail an authorisation by EU Member States' national data protection authorities to transfer EU data subjects' data abroad (Article 46(3) GDPR).[121] Such an authorisation may constitute an 'additional requirement' to be fulfilled by service suppliers established in countries that do not benefit from adequacy decisions. More generally, unlike EU service providers, those established in third countries may still need to comply with GDPR rules on cross border data transfer beyond the EU if they wish to gather Europeans' data for legitimate business interests.[122]

These GDPR restrictions for service providers of countries not benefiting from adequacy determinations may be construed as falling under the exception enshrined in Article XIV(c)(ii) GATS. This exception allows the establishment of measures 'necessary 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'. Although the 'right to regulate' stemming from Article XIV(c)(ii) GATS generally allows for protection of data privacy to limit transfer of data, such limitation should be non-discriminatory and

services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country'.

[119] S. Yakovleva and K. Irion, cit. at 116, 29; C.L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive,* 12 Melb. J. INT'L L. 141 (2011), 153–56.

[120] See for instance GATS Article SVII.1 'In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers'.

[121] F. Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements*, 2019 4 European Papers 881 (2019), 886; S. Yakovleva and K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, cit. at 117, 204.

[122] S. Yakovleva, *Personal Data Transfers in International Trade and EU Law*, cit. at 58, 893.

non-ambiguous in nature.[123] Yet, as highlighted by Kuner, the Commission at times 'prioritises discussions with third countries based on political factors' for the negotiation of adequacy decisions.[124]

Moreover, it is doubtful whether the design and the implementation of EU data protection law premised upon adequacy decisions may pass the 'least trade-restrictive' test required by WTO law when assessing Article XIV(c)(ii) GATS limitations.[125] The 'accountability approach' used in Canada can be seen as more compatible with GATS in so far as it is less restrictive on trade. As a matter of fact, the Personal Information Protection and Electronic Documents Act (PIPEDA)[126] does not distinguish between domestic or international data transfer requirements. The data exporter will respond to the accountability principle according to which the transferring organisation remains responsible for the protection of the information transferred to a third party.[127] When compared to the Canadian approach, the EU's approach thus marks more clearly the distinction between internal and external legal regimes when it comes to data transfer. This is also due to the importance that the EU attaches to the protection of its internal regulatory autonomy.

The distinctiveness of EU data protection law and its friction with the GATS scheme also emerges in comparisons with provisions on data protection and trade in different bilateral trade agreements. Other jurisdictions address data protection in a manner that is arguably more consistent with the WTO's principles. For instance, the United States-Mexico-Canada Agreement on

---

[123] N. Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020) 19 World Trade Review 341, 352.

[124] C. Kuner, 'Internet and the Global Reach of EU Law' (n 3) 136.

[125] S. Yakovleva and K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, cit. at 116, 13–14.

[126] Canada, Personal Information Protection and Electronic Documents Act (PIPEDA) (S.C. 2000, c. 5), Act current to 2021-01-10 and last amended on 2019-06-21, https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-11.html#h-417659

[127] See ibid. PIPEDA schedule 1, 4.1, 4.1.3, 4.5, and OneTrust DataGuidanceTM and Edwards, Kenny & Bray LLP, 'Comparing Privacy Laws: GDPR v. PIPEDA' 24 <https://www.dataguidance.com/sites/default/files/gdpr_v_pipeda.pdf> accessed 1 February 2021; C. Kuner, D*eveloping an Adequate Legal Framework for International Data Transfers*, in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt, (eds) *Reinventing Data Protection?*, (2009).

Trade (USMCA) contains a generic provision that preserves the parties' rights to regulate that largely mirrors the GATS exception enshrined in Article XIV(c)(ii). In fact, its Article 19.11 (2) reads:

> This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective. [128]

Differently from what happens in trade agreements concluded by other entities, in EU trade agreements, the approach is again more focused on preserving the autonomy of the EU legal order and the protection of the constitutional fabric of the EU's data privacy law. This approach stems from the fact that data protection of EU data subjects' privacy is a fundamental right. Indeed, in the new generation of trade agreements, the EU proposes clauses which aim to protect its regulatory autonomy. The provisions at issue insulate the EU data protection regime from external influences arising from its trade relations. The EU-UK TCA relevant provision reads:

> Each Party may adopt and maintain the safeguards it deems 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. *Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards*.[129]

These two approaches highlight different visions of the relationship between data protection and trade. As perceptively pointed out by Yakovleva, they are informed again by different

[128] Agreement Between the United States of America, the United Mexican States, and Canada, Can.-Mex.-U.S. (USMCA), 10 December 2019, Article 19.11(1),

[129] European Commission, 'Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements', 31 January 2018, 3 (emphasis added). See also Article 202 EU-UK TCA, cit. at 97: 'Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data' transferred.

regulatory understandings of trade in services entailing data flows. In the US, 'even when some degree of privacy and data protection *are* factored into this discourse of digital trade, the protection of these interests is often presented as an *economic* necessity, a precondition for free trade rather than a fundamental right and societal value beyond its economic utility'.[130] In this understanding, the clauses in trade agreements which possibly allow for restrictions on trade for data privacy reasons are limited and circumstantiated in their scope. In the trade agreements concluded by the EU, instead, the clauses protecting regulatory autonomy on data privacy are absolute and take the form of non-affectation clauses. In other words, while in the US trade and data privacy discourse on data protection is considered primarily in an instrumental fashion to increase consumer trust and enhance trade; in the EU, although this aspect is present,[131] the principal rationale is that of protecting and safeguarding the constitutional rights of individuals.[132]

In EU law, the attention is on whether cross-border data transfer should be allowed and under what conditions to maintain constitutional and human rights safeguards. In international trade law, instead, the attention is placed on circumscribing the cases in which transfer should be limited. [133] It is worth stressing that the absolute character of the clauses protecting data privacy and regulatory autonomy of the EU serve to insulate the specific characteristics of EU data privacy from international trade regimes.

5. Conclusions

Data protection in the EU has a constitutional nature as a fundamental right. Based on Article 8 of the EU Charter of Fundamental Rights and Article 16 TFEU, the GDPR is an expression of this. EU primary law also enshrines a mandate to

[130] S. Yakovleva, *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law* (2024), chap 3.

[131] See for instance Article 202(1) EU-UK TCA: 'Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade'.

[132] S. Yakovleva, *Governing Cross-Border Data Flows*, cit. at 130, 169-174.

[133] S. Yakovleva, *Personal Data Transfers in International Trade and EU Law*, cit. at 58, 912.

project EU law beyond EU membership.[134] The wider reach of EU data protection law reflects both the constitutional tenor of data protection in the EU and the Union's constitutional mandate to engage with foreign jurisdictions by upholding its values, interests and, ultimately, its laws. The joint combination of the wide territorial reach of EU data protection law and EU data transfer rules contribute to the nurturing of a 'domestic utopia' for EU data subjects. Such a legal construction is premised on the classical posture of EU law, which has been critically and powerfully described as a 'new legal and conceptual order' which floats above "political disorder"'.[135]Yet, in the encounter with foreign jurisdictions, EU law cannot help dealing with political realities in the international arena.[136]

There are tensions in the interface between EU data protection law and the political context. The encounter of the EU's domestic utopia with political realities beyond the EU may mitigate the global reach of EU data protection law. In *Google v CNIL*, although the full application of EU data protection law could have mandated for a global de-referencing, the political context beyond the EU and the effects of geo-blocking suggested a de-referencing in EU Member States only. Tensions between law and politics arise also in the context of data transfer. In the case of the EU-US adequacy scheme, risks of political interferences in the monitoring of the law led the CJEU to invalidate adequacy frameworks. These included shortcomings in the political independence of the bodies responsible for remedies to possible violation of data protection and the overall safeguards to data protection vis à vis the political process. In adequacy decisions, the interplay between the political and the legal is apparent from the fact that the Commission is both the 'political' negotiator of adequacy schemes and the institution in charge to monitor the adequate protection of data in foreign jurisdictions. The empowerment of EU national authorities in *Schrems I* by the CJEU could be construed as an attempt to insulate

[134] See for instance Article 3(5), Article 8 and Article 21 TEU.
[135] L. Azoulai, *Structural Principles in EU Law: Internal and External*, in M. Cremona (ed), *Structural principles in EU external relations law* (2018) 38. For a problematisation see also F. de Witte, *Interdependence and Contestation in European Integration*, 3 European Papers (2018).
[136] See also in this sense L. Azoulai, *Structural Principles*, cit. at 134.

the monitoring of the data protection law from the political process of the adequacy determinations.[137]

In the ideal global domestic utopia promoted by EU data protection law, adequacy frameworks are a way to insulate the protection of EU data subjects from different legal-political preferences and processes in foreign jurisdictions. Adequacy decisions are indicative of the deference to EU regulatory choices by third countries. As a matter of fact, especially the Japan case illustrates how adequacy decisions could be loosely compared to the disconnection clauses that the EU utilises to protect EU membership law from the relevant international regime to which the EU and /or its Member States are parties. [138]Disconnection clauses can be construed as a manifestation of the structural dimension of the principle of autonomy[139] intended to safeguard the special relationship intercurrent between the EU and its Member States from international law mechanisms. Similarly, adequacy frameworks create a special regime for EU data subjects. In that light, the insulation of the legal the regimes applicable to EU data subjects from those in place for other data subjects in foreign jurisdictions arguably appears to question the paradigm of the 'Brussels effect' premised upon a 'unilateral regulatory globalisation'.[140] Indeed, as the US adequacy saga also demonstrates, the variety of data protection arrangements promoted by the EU is somewhat resistant to change in the data protection systems of EU partners with more developed domestic

[137] L. Azoulai and M. van der Sluis, *Institutionalizing Personal Data Protection*, cit. at 56.

[138] For instance, Article 26.3 of the Council of Europe Convention on the Prevention of Terrorism signed in Warsaw on 16 May 2005 reads: 'Parties which are members of the European Union shall, in their mutual relations, apply Community and European Union rules in so far as there are Community or European Union rules governing the particular subject concerned and applicable to the specific case, without prejudice to the object and purpose of the present Convention and without prejudice to its full application with other Parties.' See further M. Cremona, *Disconnection Clauses in EC Law and Practice,* in C Hillion and P. Koutrakos (eds), *Mixed agreements revisited : the EU and its member states in the world* (2010).

[139] M. Cremona, *Structural Principles and Their Role in EU External Relations Law*, in M. Cremona (ed), *Structural principles,* in M. Cremona, cit. at. 135.

[140] A. Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev., 5.

preferences. This signals that different cultural approaches to data protection law are likely to remain.[141]

The framing of EU data protection law as a fundamental right is evident in the drafting of EU trade agreements. Such a framing stands in contrast to other approaches in trade law whereby the trade and economic considerations related to data protection are paramount. Since, EU law frameworks hardly lead to less restrictive trade arrangements,[142] some frictions may thus arise between the EU approach to data protection and the GATS.

The constitutional rigidity of EU data protection law mainly arises from the fact that limitations to data privacy in the EU can only be governed at the level of EU primary law.[143] The attempts to preserve the constitutional protection of data privacy have animated the EU's engagement to shape international law according to its values and interests: the globalisation of the Council of Europe Convention 108 is a case in point. In turn, the size and the clout of the EU market and trade opportunities are a driver for third-countries convergence to EU rules and standards.[144]

The EU's domestic utopia in data protection law, however, is emblematic of the reality deficit of EU law, which attempts to disconnect from the legal and political realities. This is reflected in the 'enforcement deficit' of the GDPR,[145] both within[146] and outside the EU.[147]The ineffectiveness of the provision of the scope of application of the GDPR (Article 3) with regard to enforcement suggests that EU data transfer rules are considered more reliable in

[141] For Japan, see F. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, cit. at 77; P.M. Schwartz, *Global Data Privacy: The EU Way,* cit. at 43.

[142] For a problematisation of the relationship between trade and protection of personal data see also M. Słok-Wódkowska and J. Mazur, *Between Commodification and Data Protection: Regulatory Models Governing Cross-Border Information Transfers in Regional Trade Agreements*, 37 Leiden J. Int'l L. 111 (2024).

[143] S. Yakovleva, *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law* (2024) ch 2.

[144] A. Bradford, *The Brussels Effect*, cit. at 4.

[145] C. Kuner, *Protecting EU Data Outside EU Borders under the GDPR*, 60 Common Mkt. L. Rev. 98 (2023).

[146] Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 International & Comparative Law Quarterly 799.

[147] B. Greze, 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9 International Data Privacy Law 109.

this respect.[148] Yet, it should be noted that the adequacy schemes of data transfer rules are hardly a complete solution for upholding the EU's values and interests abroad. It has been shown that the EU-US arrangements have been of voluntary nature, subject to the adhesion of the companies. In turn, the EU-Japan mutual adequacy framework does not cover the public sector. As the Schrems saga demonstrate, moreover, these arrangements may be invalidated by the CJEU.

In times of geopolitical fragmentation, a process of EU-wide re-bordering is occurring.[149] In data protection, this takes the form of data localisation: a preference is arising for data to remain in the EU and not be transferred beyond the Union. Several commentators put forward that the prospect of data localisation are lurked behind the *Schrems II* judgment.[150] New developments in EU digital sovereignty are thus coming to the fore whereby, as perceptively put forward by Fahey, the 'Digital Markets Act, AI Act and the Digital Services Act, combined with data localisation measures, they cumulatively could amount to a litany of measures to develop a de facto and *de jure* European firewall'.[151] The localisation trend has some of its origins in CJEU case law[152] and it is being put forward in different policy areas. Pursuant to this rebordering in data protection, in the health domain, the European Data Protection Board and the European Data Protection supervisor have suggested that the Proposal on the European Health Data Space should include an obligation 'on controllers and processors established in the EU processing personal electronic health data within the scope of the Proposal […] to store this data in the Union'.[153] The new geopolitical fragmentation is hence redesigning the balance

[148] C. Kuner, *Protecting EU Data Outside EU Borders*, cit. At 145, 97.
[149] A. Petti, *EU Membership in a Geopolitical Era*, paper presented at the Common Mkt. L. Rev. 60th anniversary conference, Leiden, June 2023, article forthcoming.
[150] Indeed, this was a solution suggested by Schrems himself after the delivery of the judgment, on this see Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23 Journal of International Economic Law 771. See more generally Christopher Kuner, 'Data Nationalism and Its Discontents' (2015) 64 Emory L. J. Online 2089.
[151] E. Fahey, *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?*, 8 European Papers 503 (2023).
[152] See for instance C-203/15, *Tele2 Sverige AB*, EU:C:2016:970, para 122.
[153] EDPB-EDPS, 'Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space', 12 July 2022, 28. See on this S. Yakovleva, *Governing Cross-Border Data Flows*, cit. at 130, 73.

between protectionism and liberalism in EU data protection law predicated on the nature of data privacy as a fundamental right which may be more difficult to uphold in foreign jurisdictions.