INSIGHT

EU STRATEGIC AUTONOMY AND TECHNOLOGICAL SOVEREIGNTY
edited by Charlotte Beaucillon *and* Sara Poli

DOES THE EU'S DIGITAL SOVEREIGNTY PROMOTE LOCALISATION IN ITS MODEL DIGITAL TRADE CLAUSES?

ELAINE FAHEY*

ABSTRACT: The EU increasingly advocates a message of tech or digital sovereignty as its future, which appears to align closely with the concept of strategic autonomy. Arguably digital sovereignty has a highly differentiated understanding in the EU as opposed to the US or China. Increasingly, many suggest EU digital sovereignty in the era of the GDPR is a high protectionist idea. Yet the EU has determined that external relations should not be at the cost of sacrificing EU data protection standards. The links of sovereignty to localisation in the context of digital trade are increasingly problematic for the EU as it seeks to reconcile high standards in the post GDPR era. The EU faced complex critique for the CJEU Schrems II ruling, for the emphasis that it places upon data localisation directly or indirectly and the manner in which it appears to awkwardly champion digital sovereignty, particularly where several EU member states practice similar levels of surveillance. The EU has developed model clauses in digital trade balancing its high GDPR standards and its external relations ambitions. The piece considers the concepts of localisation as a development of digital sovereignty in the EU's international economic law trajectory. Arguably, the model clauses here turn out to be a template of flexibility not absolutism. Whether the EU's model horizontal clauses reconciling the GDPR and international economic law goals cause difficult for future public policy or ultimately undermine the EU's goals as to liberalising data flows remains to be seen.

KEYWORDS: Digital sovereignty – Localisation – Digital Trade – CJEU – Protectionism – Data protection.

I. OVERVIEW

The expression "European technological sovereignty" refers to the process of transforming the Union into an entity capable of managing technology independently from others.[1] Such an ambitious objective arguably goes beyond that of strengthening the EU's

* Professor of Law, University of London, elaine.fahey.1@city.ac.uk.

[1] See for instance: E Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity* (Hart 2022) ch.1.

ISSN 2499-8249
doi: 10.15166/2499-8249/670

strategic autonomy and has a political and legal distinctiveness to strategic autonomy perhaps of much significance – although unclear legally, perhaps even constitutionally, as much as politically.[2] It is also said to be so complex that its constitutionalisation is increasingly problematic.[3]

The EU increasingly advocates a message of tech or digital sovereignty as its future, which appears to align closely with the concept of strategic autonomy.[4] It advocated developing the capability for the EU to make its own choices on its own values[5] and own rules as a new agenda of EU law in the era of Big Data and digitisation.[6]

Digital sovereignty is understood in EU official documents and EU Member State actors[7] and institutions[8] to warrant much law-making, arguably more internally than externally on its face.[9] Sovereignty is long the subject of controversy in the EU.[10] Historically, digital sovereignty is no less controversial in the EU.[11] Arguably digital sovereignty has a highly differentiated understanding in the EU as opposed to the US or China, particularly as to data protection law and digital trade *in the absence of global standards*. Increasingly, many suggest EU digital sovereignty in the era of the GDPR is a highly defensive and protectionist idea.[12] This "defensiveness" is legally complex to unravel for a variety of reasons. In particular, its links to localisation in the context of digital trade are increasingly discussed, which are the focus briefly of the current short piece. Data localisation measures that encumber the transfer of data across jurisdictional borders raise many

[2] D Fiott, 'Strategic Autonomy: Towards "European Sovereignty" in Defence?' (30 November 2020) European Union Institute for Security Studies www.iss.europa.eu; E Fahey and S Poli, 'The Strengthening of the European Technological Sovereignty and its Legal Bases in the Treaties' (23 May 2022) Eurojus.it rivista.eurojus.it; T Ackermann, A McDonnell, L Azoulai and others, 'Editorial Comments: Keeping Europeanism at Bay? Strategic Autonomy as a Constitutional Problem' (2022) CMLRev 313.

[3] T Ackermann, A McDonnell, L Azoulai and others, 'Editorial Comments: Keeping Europeanism at Bay?' cit. 2.

[4] Although it has older origins: V Reding, 'Digital Sovereignty: Europe at a Crossroads' (2016) EIB Institute institute.eib.org; P Grüll, '"Geopolitical" Europe Aims to Extend its Digital Sovereignty from China' (9 September 2020) Euractiv www.euractiv.com.

[5] European Commission, *Press remarks by President von der Leyen on the Commission's new strategy: Shaping Europe's Digital Future* (19 February 2020) ec.europa.eu.

[6] C Kuner, 'Data Nationalism and Its Discontents' (2015) Emory Law Journal Online law.emory.edu.

[7] Opinion of the Economic, Social and Environmental Council (France), *Towards a European Digital Sovereignty Policy* www.lecese.fr.

[8] T Madiega, 'Digital Sovereignty for Europe' (July 2020) European Parliament Research Service Ideas Paper Briefing www.europarl.europa.eu; See Resolution 2019/2575(RSP) of the European Parliament of 12 March 2019 on Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them.

[9] G De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2020) ICON 41.

[10] *E.g*. D Herzog, *Sovereignty, RIP* (Yale University Press 2020).

[11] E Fahey, *The EU as a Global Digital Actor* cit. 1.

[12] S Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (2019) World Trade Review 541; A Chander and U Lê, 'Data Nationalism' (2015) Emory Law Journal 677.

questions. Data transfers constitute one of the most significant and complex areas for the EU to attempt to engage in regulation thereof. It also traverses external relations more clearly than concepts such as digital sovereignty but is a key facet thereof.

Localisation also refers to conceptual debates in international economic law as to digital trade, the main focus of analysis here. Data localization is generally used to refer to more explicit requirement that data be stored and/or processed within the domestic territory.[13] Data localisation has been growing and is becoming increasingly restrictive globally – *i.e*. it is becoming a global problem. In 2021, there were 92 data localisation measures spread across 39 countries, with more than half having emerged in the last 5 years.[14] There are broadly speaking four key forms of national and regional policies on cross-border data flows – from strict data localisation or partial data localisation evidenced by restrictive practices in countries such as China or India or Russia, to more conditional transfer approaches understood to be "hard" *e.g*. the EU or Switzerland to conditional transfer with softer approaches *e.g*. including EU partners Japan, New Zealand, Republic of Korea to those with so called "light touch approaches" to the free flow of data *e.g*. evidenced in EU partners such as Canada, Singapore and the US.[15] This *Insight* considers how requiring that third countries respect high EU standards as to data protection in digital trade matters is considered to be protectionist, *i.e*. in the sense of restrictive and even defensive – and reflects on the variety of meanings as to localisation emerging.

The short *Insight* thus considers *i)* the framing of EU data localisation, *ii)* landmark developments in case law and frameworks on data transfers and *iii)* the EU's model horizontal clauses in digital trade and localisation clauses, followed by Conclusions.

II. On EU data localisation: On meaning, form and content

Information control is central to the survival of authoritarian regimes but also presents many economic and social benefits and challenges.

There are more actors, specifically governments, seeking to assert control over global data flows and from China to Europe and there are many important examples of control of data flows, even by third country EU partners *e.g*. India, with some of the world's most strict localisation rules.[16]

[13] N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows are Spreading Globally, What they Cost and How to Address Them' (19 July 2021) Information Technology & Innovation Foundation itif.org.

[14] J López González, F Casalini and J Porras, 'A Preliminary Mapping of Data Localisation Measures' (2022) OECD Trade Policy Papers www.oecd-ilibrary.org.

[15] *Ibid*.

[16] Yet India is the subject of a new attempt at negotiation in the form of a Council: see European Commission Press Release, 'EU-India: Joint press release on launching the Trade and Technology Council' (25 April 2022) ec.europa.eu.

The EU in 2018 sought to ban data localisation restrictions in order to ensure the free flow of data.[17] The Regulation was adopted with the intention of ensuring that the freedom to choose a data service provider anywhere in Europe would lead to more innovative data-driven services and more competitive prices for businesses, consumers and public administrations. Although on its face the Regulation had the intention to permit data to flow freely, allowing companies and public administrations to store and process non-personal data wherever they choose in the EU, there are important inhibitions on data within the territory of Europe placed here.[18] Whether it will have a more significant impact upon the understanding of localisation remains to be seen. It demonstrates the bandwidth of regulation to be immense.

Globally more attempts are made to impose structures, architecture, actors, controls, reviews and access controls around data. Data localisation is a complex phenomenon to regulate because it is about reducing access to data and digital technologies.[19] Data localisation raises the costs of access to, and use of, data.[20] Governments across the world also increasingly cite foreign surveillance as an argument to prevent data from leaving their borders.[21] Data localisation as a result can be understood as measures that encumber the transfer of data across jurisdictional borders.[22] Indeed, some of the most controversial global localisation actors are EU partners involved in close negotiations with the EU in trade and technology involving Trade and Technology Councils, *e.g*. India and the US.[23] Localisation often includes rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data. Data localisation measures are possibly likely to undermine security, privacy, economic development, and innovation where adopted.[24] Yet paradoxically, requiring local data storage arguably undermines, rather than

[17] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union; Regulation 2018/1807 was adopted as part of the Single market for data storage and processing services, such as cloud computing.

[18] The Regulation 2018/1807 removes any restrictions imposed by Member States' public authorities on the geographical location for storing or processing non-personal data, unless such restrictions are justified on grounds of public security. The Regulation defines non-personal data to include the rapidly expanding Internet of Things, artificial intelligence and machine learning.

[19] J Meltzer, 'Governing Digital Trade' (12 April 2019) World Trade Review 23, 25; See, E Fahey, *The EU as a Global Digital Actor* cit. 1.

[20] J Meltzer, 'Governing Digital Trade' cit. 25.

[21] *Ibid*. 680.

[22] A Chander and U Lê, 'Data Nationalism' cit. 12; A Chander, 'Is Data Localization a Solution for *Schrems II*?' (25 September 2020) JIEL 771.

[23] On the European Commission Press Release, 'EU-India: Joint press release on launching the Trade and Technology Council' cit. 16. On EU-US: See European Commission, 'EU-US Trade and Technology Council' (2019) ec.europa.eu.

[24] Particularly as to EU-India cooperation, where India has had strict data localisation rules.

strengthens, fundamental rights if it facilitates intelligence services to access data locally and then sharing them with other countries.[25]

Data localisation is thus highly complex and bifurcated – and also context specific. It is important then that this is viewed with caution and assessed against prevailing metrics, norms and values. With this in mind, the *Insight* next turns to consider key caselaw on data transfers.

III. The landmark transatlantic data transfer case law and framework framing soft localisation?

Landmark decisions of the CJEU in *Schrems II* are said – usually by US scholars – to mark key shifts towards data localisation in Europe.[26] In *Schrems v Data Protection Commission (Schrems I)*[27] the CJEU invalidated the EU-US Safe Harbour Agreement. The CJEU then in the Case of *Schrems II* held that the Commission's finding that US law was of an adequate level of protection essentially equivalent to EU law under the GDPR read in light of the Charter, was called into question by the surveillance programmes in section 702 FISA and E.O. 12333 because they authorised surveillance programmes such as PRISM and UPSTREAM, violating[28] the principle of proportionality. A number of US Internet companies have set up local data processing centres as a way to deal with strict European standards for instance, entailing that market pressures force location. The EU faced complex critique for the CJEU *Schrems II* ruling, for the emphasis that it places upon data localisation directly or indirectly and the manner in which it appears to awkwardly champion digital sovereignty, particularly where several EU member states practice similar levels of surveillance.[29]

The CJEU suggested using supplementary measures to protect data under the Standard Contractual Clauses (SCCs) but does not explain what these measures could be and in effect SCCs became "mini-adequacy" decisions.[30] "Soft" data localisation is thus the

[25] C Kuner, 'Requiring Local Storage of Internet Data Will Not Protect Privacy' (6 December 2013) OUP Blog blog.oup.com; C Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).

[26] Case C-311/18 *Facebook Ireland and Schrems (Schrems II)* ECLI:EU:C:2020:559; C Kuner, 'Data Nationalism and Its Discontents' cit. 6; K Propp and P Swire, 'After *Schrems II*: A Proposal to Meet the Individual Redress Challenge' (13 August 2020) Lawfare Blog www.lawfareblog.com.

[27] Case C-362/14 *Schrems (Schrems I)* EU:C:2015:650.

[28] E Fahey and F Terpan, 'Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield' (2021) IndJGlobalLegalStud 205.

[29] *Schrems II* cit. 27; A Chander, 'Is Data Localization a Solution for *Schrems II*?' cit. 24; K Propp and P Swire, 'After *Schrems II*' cit. 28; C Kuner, 'The Schrems II Judgment of the Court of Justice and the Future of data Transfer Regulation' (17 July 2020) European Law Blog europeanlawblog.eu.

[30] A Chander 'Is Data Localization a Solution for *Schrems II*?' cit. 24.

likely result there.[31] It has thus been argued that the CJEU itself does not really know what EU data localisation looks like or means in the post – *Schrems II* world.[32]

However, in March 2022, Ursula Von der Leyen and Joe Biden announced that the EU and the US had reached an agreement in principle for a new Trans-Atlantic Data Privacy Framework on the basis of which data will be able to flow freely and safely between the EU and participating US companies. It is a remarkable development which seems to elevate the plan of institutions in the protection of rights of citizens and businesses. This agreement will contain "a new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security".[33] In this context, "US intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards".[34] The agreement also includes "a new two-tier redress system to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court".[35] The effects thereof remain to be seen. They appear to deal with the complexities of *Schrems*. Yet the devil is in the detail and the extent to which CJEU concerns can be met remains a broader question in an environment where much US scepticism prevails beneath the surface about institutions in the transatlantic context. An EU review of all existing adequacy decisions – 14 at the time of writing – appears on the horizon in 2023 and highly salient going forward, albeit beyond the scope of this *Insight*. Any US-based localisation critiques of EU localisation appear to be trumped by the EU-US Data Privacy framework and even its Court- but other partners may not as comfortable with these formulations of rights, powers and institutions.

Beyond adequacy or transfer regimes, this links to the broader question in international trade law as to how the EU increasingly models data flows, data protection and rights in its digital trade chapters and how this impacts data localisation.

IV. The EU's model horizontal clauses and localisation clauses in digital trade

In recent years, many trade agreements have started to include provisions on data localisation e.g. banning or limiting requirements on the location or use of data. An important

[31] Case C-623/17 *Privacy International* ECLI:EU:C:2020:790; joined cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Other* ECLI:EU:C:2020:791; See A Chander, 'Is Data Localization a Solution for *Schrems II*?' cit. 24.

[32] A Chander, 'Is Data Localisation a Solution for *Schrems II*?' cit. 24; E Fahey, *The EU as a Global Digital Actor* cit. 1.

[33] European Commission Press Release, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (25 March 2022) ec.europa.eu; US Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (the "Order") of 7 October 2022.

[34] See the Order *Ibid.*

[35] *Ibid*.

difference with the data flows provisions is that almost all data location provisions found in trade agreements are of a binding nature.[36] Yet data localisation[37] is likely to damage cloud computing, innovation and data agility. In addition to digital services taxes, 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.[38] As a result, it is argued that EU digital protectionism is stifling and hampers trade even if it is 'soft' data localisation.[39]

The EU rejects, in principle, the assumption of an obligation to allow cross-border data flows in trade agreements. Instead, it has emerged with a solution in the form of the model horizonal clauses in digital trade. There, it argues for a form of data localisation, outlawing rules that require a company to locate its computing facilities or network in the territory of the other party or that require data to be stored or processed there. The EU also advocates giving each party an absolute right to maintain any data privacy safeguards it deems appropriate. This operates parallel to the adequacy decision process and is heavily linked – politically at least with the sequence following a trade agreement negotiation being opened and taken forward.

In the wake of the introduction of the EU's far-reaching General Data Protection Regulation (GDPR) the European Commission developed highly significant so-called model "horizontal" clauses on cross-border data flows and personal data protection in EU trade and investment agreements after pressure from the European Parliament. [40] The clauses typically provide that the EU is supportive of cross-border flows of data to facilitate trade and shall not restrict such flows through the localisation of data in the territory of the other party.[41] Most recent EU trade partners have willingly accepted the EU's clauses,

[36] M Burri and R Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' (2020) *JIEL* 187, 214.

[37] A Chander and U Lê, 'Data Nationalism' cit. 12.

[38] Communication COM (2020) 825 final from the Commission of 15 December 2020 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[39] C Barshefsky, 'EU Digital Protectionism Risks Damaging Ties with the US' (2 August 2020) Financial Times www.ft.com.

[40] European Commission Newsroom, *Horizontal provisions for cross-border data flows and for personal data protection* (18 May 2018) ec.europa.eu; Communication COM(2017) 07 final from the Commission to the European Parliament and the Council of 10 January 2017 on exchanging and protecting personal data in a globalised world.

[41] J A Micallef, 'Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?' (2019) JWT 855, 867; M Burri and R Polanco, 'Digital Trade Provisions in Preferential Trade Agreements' cit. 38; Cf Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (EU-UK TCA) [2021] (EU-UK TCA), art. 202.

with the curious and perhaps esoteric exception of the UK attempting to advocate *its* own digital sovereignty.[42]

The model clauses are understood to contain a very particular prohibition on restrictions of cross-border data flows than in so-called US models implemented in the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP), United States-Mexico-Canada Agreement (USMCA), US-Japan Digital Trade Agreement and China's model implementation of the Regional Comprehensive Economic Partnership (RCEP).[43]

In fact, it is said that the clauses are "fully" endorsed in the EU's currently and recently negotiated deals, which include in their draft digital trade chapters norms on the free flow of data and data localisation bans.[44] Third countries with no comprehensive data law have clearly had a more challenging time or been more complex to deal with. Yet this may be open to much contestation. the EU's repositioning and newer commitments are also linked with higher levels of the regulation of data protection.[45] The EU gives itself ample regulatory leeway for its current and future data protection measures. There are also broad carve-outs providing for the right to regulate.[46] The EU provides for data sovereignty of a broad nature within its recently agreed or recently negotiated clauses.[47]

Whether the EU's model clauses cause difficultly for future public policy or ultimately undermine the EU's goals as to liberalising data flows remains to be seen. However, their links to data flows and adequacy processes alongside digital trade chapters could mark a key development going forward in the concept of digital sovereignty, as a stranglehold or erosion of the fortress of EU digital sovereignty in a globalised world.

V. Conclusions

It is difficult to draw a firm conclusion at this juncture on digital sovereignty. Its protectionist dimensions are palpable. Yet it sits uneasily alongside an agenda of strategic autonomy. Ultimately, the internet appears to be likely to be further split or divided between regulatory regimes, beyond that which the EU GDPR has initiated, from the Great Firewall of China to the West of Europe.[48] Beyond the internet itself, data flows have a complex

[42] See generally the account of M Burri, 'Trade Law 4.0: Are We There Yet?' (2022) JIEL 53.

[43] See S Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of two "Necessities"' (2020) Journal of World Investment and Trade 881.

[44] *Ibid*.

[45] M Burri and R Polanco, 'Digital Trade Provisions in Preferential Trade Agreements' cit. 38; S Yakovleva, 'Personal Data Transfers in International Trade and EU Law' cit. 44; E Fahey, *The EU as a Global Digital Actor* cit. 1.

[46] See *e.g*. art. 2 of Draft EU-Australia FTA; Draft EU–New Zealand and the EU–Tunisia FTAs; M Burri, 'Interfacing Privacy and Trade' (2021) CaseWResLRev 35.

[47] M Burri, 'Interfacing Privacy and Trade' cit. 47; see also, art. 6(2) draft EU–Australia FTA, draft EU–New Zealand and the EU–Tunisia FTA.

[48] *E.g*. EU users of US websites found themselves black listed from many US sites post-GDPR introduction or have to accept acceptance of user values upon site landing: BBC News, 'European Readers still Blocked from some US News Sites' (26 June 2018) www.bbc.co.uk.

future. Localisation constitutes a valuable constitutional, political and regulatory focus point for many issues. Digital sovereignty is far from a clear idea. Similarly, localisation has manifold meanings and interpretations. Still, they are a clear marker of change in the EU as a global digital actor. Localisation clauses reflect the identity challenges of the EU as a good global actor and a somewhat more protectionist one as to the parameters of "good" here. Localisation is thus an important touchstone of debates close to international economic law and further as to digital governance and data flows, of significance to the EU as a digital actor in an era of digital sovereignty. It is, however, am emerging identify to be reflected upon further.