medialaws

Anticipazioni

Data protection[ism]*

Vincenzo Zeno-Zencovich

Data protection[ism]

Protectionism is a policy which aims at protecting domestic industries limiting – or excluding – importation of goods or provision of services from third countries. It can sometimes manifest itself by limiting exports of certain materials or products which, included in a different product, may enable third countries to compete more effectively in the exporting country or on the world market.

Given this very broad and commonly shared definition, can one speak of a current "data protectionism?"[1]. An analysis of this topic appears to be important to understand the real nature of data and their relevance not only in international trade relations but also in global geopolitics.

If one looks at the most common and historical form of protectionism, *i.e.* high import tariffs or quotas on the importation of foreign goods, one immediately understands that this cannot apply to data, for a multitude of reasons.

a) In the first place, data are non-material and therefore do not encounter any sort of customs control[2]. The mere idea of "counting" the data (by digital units, *i.e.* bytes) make very little sense, because their value does not depend on their size, but on the information they convey or are used for (data on the distribution and sales of groceries in Sweden are of practically no use in South Africa).

b) To be even more precise, the value of data is near to zero without programmes that are able to analyze them and extract the information – past, present or future – which is needed. Clearly one could, hypothetically, prevent the use of foreign data analytics in one's territory, but – setting aside the difficulties in implementing such a measure – what would be its economic sense? Would it protect the domestic digital industry?

c) But even imagining that data (whether bulk or selected) was sold as a commodity which is scarce in the domestic market (Country A does not have enough data which it needs, and therefore imports it from country B), the protectionist measure would be aimed not at protecting the domestic data industry, but at avoiding that data be collected in country A and processed in country B to be used for economic activities in country A or elsewhere. The point is that no country objects to the importation of data concerning other countries and their processing and extraction of value on its own territory. The concern – as we shall see – is not about data imports, but about data exports[3].

If one looks at the legal framework in which international trade of data could be placed, it appears very clear that the three pillars of the GATT treaty (Article I: Most

* Il presente scritto sviluppa la relazione svolta all'incontro "Verso un nuovo quadro normativo europeo: Digital Services Act, Data Governance Act e Data Act" organizzato il 12-23 aprile 2022 a Firenze dalla Fondazione CESIFIN e dalla prof.ssa Ginevra Cerrina Feroni

[1] See S.A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, in *World Trade Review,* 18, 2019, 541.

[2] «Trade in data is different from trade in goods and other services. Data are intangible, highly tradeable, and some types of data, when processed, are a public good, which governments must provide and regulate effectively» (S. A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, ivi, 543.

[3] M. Burri, *Data Flows and Global Trade Law*, in Ead. (ed.), *Big Data and Global Trade Law*, Cambridge, 2021, at 12: «The new generation of Internet controls seeks to keep information from going *out* of a country, rather than stopping it from entering the sovereign state space» [italics in the original].

Favoured Nation principle; Article III: National Treatment principle; Article XI: Elimination of quantitative restrictions) are hardly applicable to data. Not only for their non-material nature, but also because one can easily understand the difficulties of qualifying data as a like product as the difference is not in their content, but in the software that can analyze them and extract the relevant information. The same can be said for a hypothetical, but unrealistic, discrimination between imported data and domestic data «so as to afford protection to the domestic production».

As to quantitative restrictions on imports – whatever their protectionist function might be – as one has said such kind of measurements appear to be without any economic sense.

One is therefore driven out of the barren field of international trade in goods, and directed to that of international trade in services. But neither such different perspective appears to be more fruitful.

Let us assume that the service consists in the collection, storage, processing and output of data and in all the connected downstream services (*e.g.* quality control, maintenance and assistance, metering, marketing etc.).

The protectionist measure would be that of excluding third country businesses from providing such services, or limiting the number of third country providers, or the quantity (whether in terms of operations or of value) of services provided.

These services need to be carefully distinguished in their relationship with data.

1. In some cases, such services are essential – but ancillary – for the provision of a different service. The best example is that of financial services where the transaction cannot be completed without collecting storing, and processing the data of the parties involved.
2. In other cases, such services are ancillary to the correct functioning of a material product. The whole IoT world moves around the integration between a physical object and the data it collects, receives, processes and make it operate correctly. The best example is a Tesla automobile which is, substantially, a data management software applied to a bodywork and to a mechanical machinery.
3. There are then to be considered services which nearly entirely consist in the provision of certain ICT services on the basis of/in exchange for the data which is provided by the user[4].

The first case falls under the extensive legislation, both domestic and international, on the provision of such paramount services. If a country decides – and the list of such exemptions is endless – to restrict the provision of certain services – typically financial ones – the reasons are related to its financial policies (balance of payments, currency stability, protection of the domestic banking system), not to some form of data protectionism.

The second case can be divided in two further sub-cases. That in which the protectionist measure (high tariffs, quotas) is introduced to protect domestic industry of a like product (*e.g.* refrigerators, industrial robots) which uses – like practically all nowa-

[4] See also the classification proposed by S. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?,* cit., 568, who lists five types of data: Personal data, Confidential business data, Public data, Metadata, Machine-to-machine communication.

days – IoT technologies. In this sub-case data are not at the center of the trade issue. In the other sub-case, the protectionist measure is taken not because one wants to protect the domestic industry in the like product, but because one wishes to control the use of the data. The limitation therefore has to do with compliance with domestic data legislation and especially with provisions concerning the transfer of data to third countries. Hypothetically such transfer could be completely independent from the provision of the service (which is assured by digital technologies operating in the country of importation), but is considered, very simply, an informational asset of the business, to which it is entitled.

A similar situation presents itself in the third case, where data collection, storage, and processing are the core of the business of the services of the business, which commonly is designed as a data company.

Although it is quite common to identify such companies in the two internet giants such as Facebook and Google, one should point out that there are hundreds, if not thousands, of other companies who operate on a similar business model: they provide a service on the basis of/in exchange of data. It is sufficient to take a look at the dozens of applications every user downloads on his or her computer (Adobe, anti-virus, etc) or smart-phone (maps, weather, entertainment, etc.) to realize the vastity of the phenomenon.

Again, the protectionist measure is aimed at ensuring compliance with domestic regulations on data processing and limiting the transfer abroad of data.

If one places all these cases within the context of the GATS Treaty (and not considering its very poor performance over the last 25 years, which borders irrelevance) one realizes that its provisions do not seem to apply to services which include, to a varying extent, data collection, storage and processing[5].

At any rate, one could find various provisions in the GATS Treaty which appear to justify restrictive policies. In the first place, the principle of non-discrimination is not violated if the restrictions to the transfer or data apply to any business, whether domestic or foreign (Articles VI and XVIII). In the second place, Article III bis (Disclosure of Confidential Information) and Article XIV (General Exceptions) appear to justify such measures. In particular, the latter provision expressly states that «nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures (…) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (…)

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts».

To sum up what has been so far presented, it would seem that both the GATT and the GATS Treaties, with their countless annexes, do not appear to be relevant in case of what has been, *ex hypothesis*, described as data protectionism.

The reasons of such meagre result do not depend on a defective or obsolete drafting

[5] «GATS is not sufficiently adaptable to a data-driven economy» (A.D. Mitchell - N. Mishra, *WTO Law and Cross-Border Data Flows: An Unfinished Agenda*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 93)

of the two texts, but on the very nature of data and their role in global economy and geopolitics.

On the one hand one has pointed out that data, as a non-material entity appear difficult to regulate. Their sheer quantity – which by rule-of-thumb is calculated in zettabytes –, their constant, *ad infinitum*, production, their ubiquity, the ease in reproduction and transfer render data an *unicum* in the history of mankind. For this reason, the definition of datasphere – in which data circulate with little or no control – appears to be appropriate[6]. Surely data economics are an essential part of today's economy, but precisely for this reason they need to find an appropriate classification.

Just as in any business – since the most ancient times – information (extracted from the available data) is an essential element and is variously protected (confidentiality agreements, trade-secrets, know-how), in any country the data concerning whatever happens in it concerning its territory, its entities, its citizens have a strategic importance. Just as States claim sovereignty over their land, their skies, their territorial waters, they extend such sovereignty to the non-material world of data.

The reasons for this expansion are far from trivial.

In the first place there are security concerns. Data provide sensitive information concerning the localization, nature and efficiency of security facilities. But even more, they reveal qualities and fragilities of the data transmission infrastructures, which, *per se*, are critical in any national security assessment. Cybersecurity becomes therefore a foremost goal to be advanced through the control of the data processing servers[7].

But even if one looks at the data produced in/by a country from a purely economic perspective, knowledge of such data, in a predictive analytics context, reveals the general situation, societal and economic trends, imminent crisis, foreseeable strategies. Those who hold such information data have an informational advantage which can be easily exploited. One could divide countries between "data empires" and "data colonies", and very few are happy to fall in the latter category[8].

This is the ultimate reason for "data protectionism". The aim is that of protecting not a domestic industry but national sovereignty[9]. A country that allows free access to its data resources could be compared to a country that allows the exploitation of its natural resources only to buy them back once they have been processed.

Once one has outlined the rationale of data protectionism and withholding any value judgement on its desirability or effectiveness, it is important to lay out the ways through which this policy is implemented.

---

[6] See J-S.Bergé - S. Grumbach - V. Zeno-Zencovich, *The 'Datasphere',Data Flows beyond Control, and the Challenges for Law and Governance*, in *EJCL&Gov.*, 5, 2018, 144.

[7] See P. Swire - D. Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity*, in *ssrn.com,* 2022.

[8] «Digital colonialism is traditional colonialism revisited» (A. Bhatt, *Data Sovereignty: The Quintessential Model for the New World Order*, in *Indian Law Institute Law Review,* 6, 2021, 285, at 287. And see now S. Grumbach, *L'empire des algorithmes*, Paris, 2022).

[9] Acccording to H. Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms,* in *ssrn.com,* 2021, the three great economic regions (US, RPC and EU) champion, respectively, the sovereignty of the firm, of the state and of the individual. This paper argues that, at the end of the day, all three models strive to ensure sovereignty of the state.

The first is that is commonly called "data localization"[10]. The term indicates that data collected in a certain country may be stored and processed only in that country. This means that the data may not be transferred abroad.

In this case there is no limitation to who is providing this service – and therefore there is no discrimination in access to the market of data processing services[11] – but "simply" the obligation not to transfer such data abroad.

Data localization is labelled as being against free trade, and one finds several international instruments which explicitly prohibit such practice. But if one looks at the rule in a pragmatic way, free flow of data is not really about trade[12].

Data is not sold, nor bought. Data is simply a resource on which to develop economic and marketing strategies.

The service *per se*, consisting in collecting, storing and processing data, is in no way prevented. The parallel could be that – very common in the past – of prohibiting the export of profits made by a foreign company operating in a third country. This practice is expressly prohibited by Article VIII of the IMF Treaty, but this points out that an international agreement is required to impose free flow of data[13]. If it is lacking, it is doubtful whether one can claim some violation of the very vast and consolidated international trade system[14]. In a few words: data localization is aimed at protecting national interests and, provided it is not discriminatory, it does not appear to violate international trade law[15].

An indirect way of imposing data localization is that adopted by the European Union with its pervasive personal data regulation.

One should point out that the notion of "personal data" is established by the EU and Member States institutions (CJEU, EDP Supervisor, EDP Board, National Data Protection Authorities) and is expansive, encompassing more and more data. The truth is that practically all data is "personal data" in the sense that it leads to identifiable

[10] For a wide survey and analysis of the various data localisation measures and their rationale see H. Ursic - R. Nurullaev - M. Olmedo Cuevas - P. Szulewski, *Data localisation measures and their impacts on data science*, in in V. Mak - E. Tjong Tjin Tai - A. Berlee (eds.), *Research Handbook in Data Science and the Law*, Cheltenham – Northampton (MA), 2019, 322

[11] But consider that certain researches indicate that «the establishment of local data centres does not appear to lead to new jobs created in the country» (M.F. Ferracane, *The Costs of Data Protectionism*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 70).

[12] See, however, the economic analysis by S. R. Potluri - V. Sridhar - S. Rao, *Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach*, in *Telecommunications Policy*, 44(9), 2020, according to whom «there is often clustering of consumers around local firms in highly restrictive data localisation regimes, thus enabling local firms to effectively compete against global multinationals. However, results also indicate that while free cross-border data ow enables intense competition amongst producers, data localisation restrictions often limit consumer choice due to its effect on price and quality of services».

[13] See the lengthy paragraph devoted by M. Burri, *Data Flows and Global Trade Law*, cit., 24 ss., to data-related rules in Preferential Trade Agreements (PTAs); and M. Elsig - S. Klotz, *Data Flow-Related Provisions in Preferential Trade Agreements*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 42.

[14] I have tried to present the argument in more detail in V. Zeno-Zencovich, *Free-Flow of Data. Is International Trade Law the Appropriate Answer?*, in F. Fabbrini - E. Celeste - J. Quinn (eds.), *Data Protection Beyond Borders*, Oxford, 2021, 173.

[15] M.F. Ferracane, *The Costs of Data Protectionism*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 76, presents a similar arguments more elegantly: «The debate on whether data restrictions represent a trade barrier that could potentially be challenged at the WTO is, however, still in its infancy».

natural persons[16]. The only data that would appear to fall outside the definition of the "data subject" given by Article 4, para. 1, of the GDPR, are those concerning the weather or other natural phenomena and aggregated statistical data. And the fact that the GDPR expressly limits its scope to natural persons, does not liberalize processing of data by legal entities in B2B relations, because the businesses would have to previously delete all the data concerning the natural persons involved in the transaction (the legal representative of another entity, the contact person, etc.). A very costly operation, which – coupled with the draconian sanctions imposed with the greatest of ease by the various authorities – is, in substance, discouraged.

Once one has established that practically all data are "personal data", the further step is that of prohibiting transfer of data to third countries which do not ensure «an adequate level of protection» (article 45 GDPR). And when one looks at the criteria used in article 45, para 2, to assess the «adequacy of the level of protection» it is difficult to find more than half a dozen countries, among the remaining 166 members of the UN, that pass muster. The best evidence is the inglorious fate of the "*Safe Harbour*" and of the "*Privacy Shield*" agreements of the EU with its most important political and economic partner, the US, both struck down by the EU Court of Justice[17]. A similar effect had already been achieved by the CJEU famous *Google Spain*[18] decision when it stated that the mere collection of commercial ads in a Member State was tantamount to be established in the EU, and therefore Google was considered subject to EU data protection laws.

The result is, *de facto*, a data localization principle, which is reaffirmed in the hoard of new "Digital Acts" proposals, to which one should add the very strong political pressure for the creation of an "European Cloud", which in its mere denomination implies a localization principle[19].

Setting aside comments on the rather hypocritical preach good and scratch bad approach to free flow data, one easily understands that under the cloak of fundamental rights (personal data protection enshrined in Article 8 of the EUCFR) there is the quite understandable need to avoid that the EU become even more a colony of ICT super-powers, the US and the RPC.

---

[16] Quite appropriately M. Burri, *Data Flows and Global Trade Law*, cit., reminds us (at 14) that «in reality it is now rare for data generated by user activity to be completely and irreversibly anonymized« and that «big data enables the reidentification of data subjects by using and combining datasets of non-personal data, especially as data is persistent and can be retained indefinitely with the presently available technologies».

[17] See G. Resta, - V. Zeno-Zencovich (eds.), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"* , Rome, 2016.

[18] See G. Resta - V. Zeno-Zencovich (eds.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Rome, 2015.

[19] See the 15 October 2020 Declaration by the 27 Member States on "Building the next generation cloud for businesses and the public sector in the EU": «Cloud computing provides the data processing capacities required to enable data-driven innovation, hence the urgent need to cooperate to foster Europe's technological sovereignty and to ensure that our businesses and public sector have access to resilient and competitive data storage and processing capacities. Europe's leadership in this area is essential to enable artificial intelligence, Internet of Things and 5G/6G. Europe should aim to set global norms on data storage and processing and to maintain market openness and international cooperation».

In the dualism empire/colony one can read the coherent and constant US policy against data localization which one finds in most of the international trade treaties it has promoted over the last 20 years and in innumerous policy statements.[20] The reasons are quite obvious: The US are the leaders in data processing and the "Big Data revolution" started in the US. Its digital industry is a world leader and has all the interest in broadening its market, both for collecting data and for selling the results of their analytics[21]. For the moment being they do not appear to fear that their data be collected and processed in third countries. Their main technological competitor being the RPC the action taken has been that of challenging "back-door" access to data through Chinese technology (*e.g.* Huawei). This substantially introduces a localization principle, preventing transfer of data to certain countries. As to Europe the US response to the territoriality principle of the GDPR has been the so-called CLOUD Act[22] which enables US authorities to access data held by any US company or affiliate wherever in the world.

The tit-for-tat approach in data control is manifest in the EU response to the US worldwide access. The "free flow" of non-personal data Regulation applies to any provider even if not established in the EU[23]. The Digital Services Act proposal (DSA) imposes on providers of intermediary services that are established in a third country and offer services in the EU to designate a legal representative in the Union and provide all the information on their legal representatives[24]. The proposed Artificial Intelligence Act explicitly extends its rules to providers and users of AI Systems that are established in a third country if their results are used in the EU[25].

---

[20] See, *ex multis*, Chapter 19 of the 2019 US-Mexico-Canada Trade Agreement (USMCA), according to which «No Party shall require a covered person to use or locate computing facilities in that Party ' s territory as a condition for conducting business in that territory». One finds similar provisions in the most recent trade agreements signed by the US.

[21] See S.A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, cit., 549.

[22] HR 4943 – Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (available at the US Congress website *congress.gov*). According to § 2713 «A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States».

[23] Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, Article 2: «This Regulation applies to the processing of electronic data other than personal data in the Union, which is:
(a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union».

[24] Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Article 11: «Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person as their legal representative in one of the Member States where the provider offers its services».

[25] Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 2: «This Regulation applies to:
(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
(b) users of AI systems located within the Union;
(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union».

The Data Governance Act proposal states that judgments of courts or administrative authorities of third countries requiring access to non-personal data should be enforceable only if there is an international agreement in that sense[26].

The Data Act proposal repeats such principle adding, significantly, that the provision is imposed to protect not only fundamental rights of EU citizens but also national security, intellectual property rights, trade secrets, commercial confidentiality[27].

* * * *

The analysis conducted in the previous pages brings to conclude that "data protectionism" has much more to do with international politics than with international trade. In this sense it can be associated with the never-ending saga of Foreign Direct Investments, at times invoked as a blessing, in others seen as a curse, and which sways between very substantial incentives and rigorous vetoes. In the latter case what is at stake is the industrial or financial sovereignty of a country. With data – owing to their polyfunctionality and non-materiality – the concern covers the entire spectrum of public and private activities.

This does not imply downplaying the economic relevance of free flow of data, but points out that the solution can be found only in new and shared principles enshrined in international law agreements[28]. Which, for the very troubled times we are all experiencing, appears to be wishful thinking[29].

[26] Regulation on European data governance (Data Governance Act), Article 30: «Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter 2, a data sharing provider or entity entered in the register of recognised data altruism organisations to transfer from or give access to non-personal data subject to this Regulation in the Union may only be recognised or enforceable in any manner if based on an international agreement».

[27] Regulation on harmonised rules on fair access to and use of data (Data Act), Article 27, para. 3: A EU competent authority will decide «when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States».

[28] S. A. Aaronson, *Data Is Different, Policymakers Should Pay Attention to Its Governance*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 359: «The world is awash with data and there is no consensus on how to regulate it».

[29] M. Burri, *Data Flows and Global Trade Law*, cit., 14: «The striking divergences both in the perceptions and the regulation of privacy protection across nations and in particular between the fundamental rights approach of the EU and the more market-based, non-interventionist approach of the United States have also meant that conventional forms of international cooperation and an agreement on shared standards of data protection have become highly unlikely». And her conclusive words: «Data issues cannot be covered by the mere 'lower tariffs, more commitments' stance in trade negotiations but entail the need for reconciling different interests and the need for oversight. In this context, while the paths for engaging in and advancing regulatory cooperation would ideally be followed in the multilateral forum, preferential trade venues can serve as governance laboratories. The way forward may be truly bright but remains highly (and perhaps unfortunately so) dependent on the role that the key players, the United States, the EU and China, are willing to assume» (at 41).