The CJEU Shrems cases – Personal Data Protection and International Trade Regulation

Carmen Otero García-Castrillón, Complutense University of Madrid, has kindly provided us with her thoughts on personal data protection and international trade regulation. An extended version of this post will appear as a contribution to the results of the Spanish Research Project lead by E. Rodríguez Pineau and E. Torralba Mendiola "Protección transfronteriza de la transmisión de datos personales a la luz del nuevo Reglamento europeo: problemas prácticos de aplicación" (PGC2018-096456-B-I00).

The regulatory scenario

1. In digital commerce times, it seems self-evident that personal data protection and international trade in goods and services are intrinsically connected. Within this internet related environment personal data can be accessed, retrieved, processed and stored in a number of different countries. In this context, the legal certainty for economic actors, and even the materialisation or continuation of commercial transactions requires taking into consideration both, the international jurisdiction and the applicable law issues on the one hand, and the international trade regulations covering these commercial transactions on the other hand.

Too much personal data protection can excessively restrict international trade, especially in countries with less developed economies for which the internet is considered an essential sustainable development tool. Little protection can prejudice individual fundamental rights and consumers' trust, negatively affecting international trade also. Hence, some kind of balance is needed between the international personal data flux and the protection of these particular data. It must be acknowledged that, summarising, whilst in a number of States personal data and their protection are fundamental rights (expressly in art. 8 CFREU, and as a part of the right to private and family life in art. 8 ECHR), in others, though placed in the individual's privacy sphere (in the light of art. 12 UDHR), it is

basically associated to consumer's rights.

2. The only general international treaty specifically dealing with personal data protection is the Convention 108 + of the Council of Europe, for the protection of individuals with regard to the processing of personal data. The Convention defines personal data as any information relating to an identified or identifiable individual (art. 2.a) without an express and formal recognition of its fundamental right character. The Convention, whose *raison d'etre* was justified for need to avoid that the personal data protection controls interfere with the free international flow of information (Explanatory Report, para. 9), "should not be interpreted as a means to erect non-tariff barriers to international trade" (Explanatory Report, para. 25). Its rules recognise the individual's rights to receive information on the obtaining and the treatment of their data, to be consulted and oppose that treatment, to get the data rectified or eliminated and to count, for all this, with the support of a supervisory authority and judicial and non-judicial mechanisms (arts. 8, 9 and 12). On the basis of these common standards, member States agree not to prohibit or subject to special authorisations the personal data flows as long as the transfer does not imply a serious risk of circumventing them (art. 14). Moreover, the agreed rules can be exempted when it is a "necessary and proportionate" measure "in a democratic society" to protect individual rights and "the rights and fundamental freedoms of others", particularly "freedom of expression" (art. 11). Presently, 55 States are parties to this Convention, including the EU but not the US, that have an observer status.

Along these lines, together with other Recommendations, the OECD produced a set of *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (11.7.2013; revising the 1980 version). After establishing general principles of action as minimum standards, it was concluded that the international jurisdiction and the applicable law issues could not be addressed "at that stage" provided the "discussion of different strategies and proposed principles", the "advent of such rapid changes in technology, and given the non-binding nature of

the Guidelines" (Explanatory Memorandum, pp. 63-64).

On another side, the World Trade Organisation (WTO) administers different Agreements multilaterally liberalising international trade in goods and services that count with its own dispute settlement mechanism. In addition, States and, of course, the EU and the US, follow the trade bilateralism trend in which data protection and privacy has begun to be incorporated. Recently, this issue has also been incorporated into the WTO multilateral trade negotiations on e-commerce.

CJEU Schrems' cases

3. Last 16 July, in *Schrems II* (C-311/18), the CJEU declared the invalidity of the Commission Decision 2016/1250 on the adequacy of the protection provided by the Privacy Shield EU–US, aimed at allowing the personal data transfer to this country according to the EU requirements, then established by Directive 95/46 and, from 25 May 2018, by the Regulation 2016/679 (GDPR). On the contrary, Commission Decision 2010/87 (2016/2297 version) on the authorisation of those transfers through contractual clauses compromising data controllers established in third countries is considered to be in conformity with EU law.

In a nutshell, in order to avoid personal data flows to "data heavens" countries, transfers from the EU to third States are only allowed when there are guarantees of compliance with what the EU considers to be an adequate protective standard. The foreign standard is considered to be adequate if it shows to be substantially equivalent to the EU's one, as interpreted in the light of the EUCFR (*Schrems II* paras. 94 and 105). To this end, there are two major options. One is obtaining an express Commission adequacy statement (after analysing foreign law or reaching an agreement with the foreign country; art. 45 GDPR). The other is resorting to approved model clauses to be incorporated in contracts with personal data importers, as long as effective legal remedies for data subjects are available (art. 46.1 and 2.c GDPR). According to the Commission, this second option is the most commonly used (COM/2020/264 final, p. 15).

4. In *Schrems II* the CJEU confirms that, contrary to the Privacy Shield Decision, the US data protection regime is not equivalent to EU's one because it allows public authorities to access and use those data without being subject to the proportionality principle (para. 183; at least in some surveillance programs) and, moreover, without recognising data owners their possibility to act judicially against them (para. 187). It never rains but what it pours since, in 2015, a similar reasoning led to the same conclusion in *Schrems I* (C-362/14, 5.6.15) on the Safe Harbour Decision (2000/520), preceding the Privacy Shield one. Along these lines, another preliminary question on the Privacy Shield Decision is pending in the case *La cuadrature du net,* where, differing from *Schrems II*, its compatibility with the CFREU is expressly questioned (T-738/16). In this realm, it seems relevant noting that the CJEU has recently resolved the *Privacy International* case, where, the non-discriminated capture of personal data and its access by national intelligence and security agencies for security reasons, has been considered contrary to the CFREU unless it is done exceptionally, in extraordinary cases and in a limited way (C-623/17, para. 72). Given the nature of the issue at hand, a similar Decision could be expected in the *La cuadrature du net* case; providing additional reasons on the nullity of the Privacy Shield Decision, since it would also contravene the CFREU. Moreover, all this could eventually have a cascading effect on the Commission's adequacy Decisions regarding other third States (Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Faeroe Islands, Andorra, Israel, Uruguay, New Zealand and Japan).

5. As to the contractual clauses, beyond confirming the Commission analysis on their adequacy in this case, the CJEU states that it is necessary to evaluate the data access possibilities for the transferred country public authorities according to that country national law (para. 134). At the end of the day, EU Data Protection authorities have to control the risks of those authorities' actions not conforming with EU standards, as much as the capability of the contractual parties to comply with the contractual clause as such. If the risk exists, the transfers have to be prohibited or

suspended (para.135).

6. The EU personal data protection norms are imperative and apply territorially (art. 3 GDPR; Guidelines 3/18 EDPB version 2.1, 7.1.2020 and CJEU C-240/14, *Weltimmo*). Therefore, data "imports" are not regulated and the "exports" are subject to the condition of being done to a country where they receive EU equivalent protection. In the light of CJEU case law, the measures to watch over the preservation of the EU standard are profoundly protective, as could be expected provided the fundamental rights character of personal data protection in the EU (nonetheless, many transfers have already taken place under a Decision now declared to be void).

Hence, once a third country legislation allows its public authorities to access to personal data -even for public or national security interests- without reaching the EU safeguards level, EU Decisions on the adequacy of data transfers to those countries would be contrary to EU law. In similar terms, and despite the recent EDPB Recommendations (01 and 02/20, 10.11.2020), one may wonder how the contracts including those authorised clauses could scape the prohibition since, whatever the efforts the importing parties may do to adapt to the EU requirements (as Microsoft has recently announced regarding transfers to the US; 19.11.2020), they cannot (it is not in their hands) modify nor fully avoid the application of the corresponding national legislation in its own territory.

As a result, the companies aiming to do business in or with the EU, do not only have to adapt to the GRDP, but not to export data and treat and store them in the EU (local facilities). This entails that, beyond the declared personal data international transferability (de-localisation), *de facto*, it seems almost inevitable to "localise" them in the EU to ensure their protection. To illustrate the confusion created for operators (that have started to see cases been filed against them), it seems enough to point to the EDPB initial reaction that, whilst implementing the *Strategy for EU institutions to comply with "Schrems II" Ruling*, "strongly encourages … to avoid transfers of personal data towards the United States for

new processing operations or new contracts with service providers" (Press Release 29.10.2020).

Personal data localisation and international trade regulation

7. There is a number of national systems that, one way or another, require personal data (in general or in especially sensitive areas) localisation. These kinds of measures clearly constitute trade barriers hampering, particularly, international services' trade. Their international conformity relies on the international commitments that, in this case, are to be found in the WTO Agreements as much as in the bilateral trade agreements if existing. The study of this conformity merits attention.

8. From the EU perspective, as an initial general approach it must be acknowledged that, within the WTO, the EU has acquired a number of commitments including specific compromises in trans-border trade services in the data process, telecommunication and (with many singularities) financial sectors. Beyond the possibility of resorting to the allowed exceptions, the "localisation" requirement could eventually be infringing these compromises (particularly, arts. XVI and/or XVII GATS).

Regarding EU bilateral trade agreements, some of the already existing ones and others under negotiation include personal data protection rules, basically in the e-commerce chapters (sometimes also including trade in services and investment). Together with the general free trade endeavour, the agreements recognise the importance of adopting and maintaining measures conforming to the parties' respective laws on personal data protection without agreeing any substantive standard (i.e. Japan, Singapore). At most, parties agree to maintain a dialog and exchange information and experiences (i.e. Canada; in the financial services area expressly states that personal data transfers have to be in conformity with the law of the State of origin). For the time being, only the Australian and New Zealand negotiating texts expressly recognise the fundamental character of privacy and data protection along with the freedom of the parties to adopt protective

measures (international transfers included) with the only obligation to inform each other.

Concluding remarks

9. As the GDPR acknowledges "(F)lows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data." (Recital 101). In facing this challenge, *Schrems II* confirms the unilaterally asserted extraterritoriality of EU personal data protection standards that, beyond its hard and fully realistic enforcement for operators abroad, constitute a trade barrier that could be eventually infringing its WTO Agreements' compromises. Hence, in a digitalised and globally intercommunicated world, the EU personal data protection standards contribute to feeding the debate on trade protectionism. While both the EU and the US try to expand their respective protective models through bilateral trade agreements, multilaterally -among other initiatives involving States and stakeholders, without forgetting the role of technology (*privacy by design*)- it will be very interesting to see how the on-going WTO negotiations on e-commerce cover privacy and personal data protection in international trade data flows.