From Safe Harbour to Privacy Shield. The “medieval” sovereignty on personal data

CEDAM

ISSN 1127-2872

Pubblicazione semestrale
Anno XXI

1/2016

Contratto e impresa/Europa

RIVISTA FONDATA DA F. GALGANO E M. BIN

Diretta da
da Marino Bin e Giammaria Ajani

- Sviluppi del diritto economico europeo
- Convenzione di Vienna e diritto europeo della vendita
- Contratto internazionale d'appalto
- Commercio elettronico in Russia
- Mercato finanziario: direttiva AIFM; UNIDROIT e titoli detenuti da intermediari
- Associazionismo sportivo dilettantistico
- Accordi prematrimoniali di divorzio
- L'arbitrato in Cina
- La riforma del *Code civil* in Francia
- Marchio europeo
- *Privacy:* il caso *Safe Harbour*
- Novità normative in Spagna

edicolaprofessionale.com/CIE

Wolters Kluwer

Tariffa R.O.C Poste Italiane s.p.a.- Sped. in abb. post. - D.L. 353/2003 (conv. in L. 27/02/2004 n°46) art. I, comma I, DCB Milano

From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data

1. – *Introduction*

The European Commission has defined a new agreement for the trans-border data flows from the European Union to the U.S. (1), sixteen years after the Safe Harbor agreement (2), following the Edward Snowden's revelations (3) and a few months after the ECJ ruling on the Schrems case.

The first comment might be positive, because personal data, the digital sap of our economy, is flowing again through the Atlantic. The European Commission has achieved a compromise that has highlighted the strength of the E.U. data protection model. Moreover, the forthcoming E.U. regulation (General Data Protection Regulation) will safeguard the data of European citizens. We can conclude that "all's well that ends well", according to the Shakespearean (and Italian) proverb. Nevertheless, the actual situation of the trans-border data flows looks different from this rosy forecast.

If we look at the details concerning both the E.U.-U.S. agreement and the broader topic of the international strength of the E.U. data protection model, many elements suggest a more cautious optimism.

Like a sort of medieval town, the E.U. common framework on data protection has created a legal wall around the information concerning European citizens and only a few legal gateways give access to the valuable asset represented by personal data. These include international bilateral agreements (such as the Safe Harbor agreement and the new Privacy Shield), standard contractual clauses, foreign regulations that provide adequate levels of protection, binding corporate rules, and *ad hoc* contractual clauses.

---

(1) See EUROPEAN COMMISSION, Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, draft and related Annexes. Available at *http://europa.eu/rapid/press-release_IP-16-433_en.htm* (accessed 29 February 2016).

(2) See 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 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). Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000-D0520:EN:HTML* (accessed 5 February 2016).

(3) See EUROPEAN PARLIAMENT, 2014.

In this light, the recent ruling of the judge of the "town" (the European Court of Justice) stated that one of these gateways was not secure enough (weak enforcement of the Safe Harbour principles, lack of judicial protection for EU citizens, potential risks due to the public/private surveillance partnership) and temporarily closed it. Foreigners, who want to have access to the gold of the town (i.e. our personal information), clamoured for the re-opening of the gateway. Now, a new smaller gateway has replaced the previous one and access is possible through more restrictive conditions and only under the careful watch of different guards (data protection authorities [4], ECJ, European Commission).

2. – *From Schrems to Privacy Shield*

Without metaphors, the Schrems case seems to reaffirm the strength of the E.U. legal barrier that protects personal data. However, it actually unveils the frail nature of this regulatory wall.

The ECJ judgment highlights that, according to Article 25 (6), third countries should provide "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union" [5]. In these terms, the ECJ decision does not only affect the Safe Harbour agreement, but also the new Privacy Shields and, above

---

[4] The Article 29 Working Party will publish its opinion on the Privacy Shield on April 13. The Article 29 Working Party is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC and composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. According to the Directives 95/46/EC and 2002/58/EC, this body is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents. As the ECJ has recently pointed out in the case C-362/14, *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd*, 6 October 2015 (see paras 102 and 103), the data protection authorities may autonomously "call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals".

[5] See European Court of Justice, C-362/14 (fn. 4), para 73: "The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter".

all, all the different legal grounds for data transfers outside the EU borders (i.e. third country regulations, standard contractual clauses, binding corporate rules). From this perspective, the strength of the E.U. model seems to be more formal than substantive.

Regarding the U.S., the previous experience of the Safe Harbour agreement does not appear to be particularly positive in terms of efficacy and enforcement (Connolly, 2013; Chester, 2014 (6)). When Safe Harbour was established, the Federal Trade Commission committed to review on a priority basis all referrals from E.U. Member State authorities, but no complaints were received for the first ten years. Consequently, the FTC decided to identify any Safe Harbour violations in all privacy and data security investigations it conducted. Between 2009 and 2013, the FTC has brought 10 enforcement actions against companies based on Safe Harbour violations (European Commission, 2013). After the critical remarks expressed by the European Commission about the Safe Harbour agreement (7), the number of FTC decisions concerning Safe Harbour violations increased (28 in 2014, 15 in 2015) (8), but it seems far below the real

(6) Jeff Chester, executive director del Center for Digital Democracy, declared that "Instead of ensuring that the U.S. lives up to its commitment to protect EU consumers, our investigation found that there is little oversight and enforcement by the FTC. The Big Data-driven companies in our complaint use Safe Harbor as a shield to further their information-gathering practices without serious scrutiny. Companies are relying on exceedingly brief, vague, or obtuse descriptions of their data collection practices, even though Safe Harbor requires meaningful transparency and candor. Our investigation found that many of the companies are involved with a web of powerful multiple data broker partners who, unknown to the EU public, pool their data on individuals so they can be profiled and targeted online".

(7) See EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU* (fn. 10). See also EUROPEAN PARLIAMENT, *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* (fn. 2).

(8) Since there are not official stats about the FTC decisions concerning Safe Harbor violations, the number of cases has been extracted from the FTC press releases available at the following addresses: *https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed*; *https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international*; *https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its*; *https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor*; *https://www.ftc.gov/news-events/press-releases/2014/02/ftc-settles-childrens-gaming-company-falsely-claiming-comply; https://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply*.

number of the companies that have falsely claimed to comply with the Safe Harbor framework (Connolly, 2013 [9]).

With respect to the remaining legal grounds, the main concerns deal with third country regulations and standard contractual clauses. Regarding the decisions adopted by the European Commission on the adequacy of the protection of personal data in third countries, [10] there is no evidence about how the European authorities monitor the effective enforcement of third country data protection regulations and whether they monitor and review the amendments to these regulations and related practices.

As regards the standard contractual clauses, it should be pointed out that clause II (c) of the Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) [11] requires the data importer to warrant that "It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws" [12]. Therefore, the adoption of the standard clauses does not exclude *per se* any assessment of the level of protection provided by the third country. Moreover, according to this clause, the E.U. data exporters should stop any data transfer

---

[9] In 2008, Galexia found that 208 organisations were making false claims of Safe Harbor membership. In the 2010 update, the figure was 331 and in 2013 it was 427.

[10] The list of the Commission decisions on the adequacy of the protection of personal data in third countries is available at the following address: *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm* (accessed 2 February 2016).

[11] See EUROPEAN COMMISSION, Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. C(2004) 5271. 2004/915/EC. Annex SET II. See also EUROPEAN COMMISSION, Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. C(2004) 5271. 2004/915/EC, Annex, clause 5(a).

[12] See the analogous wording of the EUROPEAN COMMISSION, Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. 2010/87/EU. Annex, clause 5(b) ("[The data importer agrees and warrants:] that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract").

or provide further safeguards when they are aware that the foreign regulations may have a "substantial adverse effect" on the guarantees provided for under these clauses (Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, 2015). Nevertheless, the standard clauses are often used by E.U. companies adopting a "copy & paste" approach, without any assessment of the mandatory rules that may affect the compliance of third parties that are based outside the E.U.

Finally, with regard to the new Privacy Shield, the legal framework is still uncertain. Although, a different and more collaborative approach is evident on the other side of Atlantic (13), the new agreement is mainly the result of a political agreement between the European Commission and the U.S. counterparts, in which the European Data Protection Authorities (hereafter DPAs) have not been directly involved.

This kind of negotiation is carried out by the Commission. However, it is the DPAs that have to examine any claims concerning personal data transfers to a third country, when the data subject contends that the law and practices in force in this country do not ensure an adequate level of protection. In these cases, when the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are well founded, that authority must be able to engage in legal proceedings.

According to the Schrems ruling, "it is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity".

Therefore, if the European DPAs are not convinced of the level of protection provided by the new agreement, they may begin a new lawsuit that leads to a new ECJ preliminary ruling on the E.U.-U.S. data transfer agreement (14). For these reason, the Privacy Shield is still "*sub judice*"

---

(13) The intention to provide a more effective protection of EU citizens' rights concerning personal information is evident not only in the new agreement, but also in the approval of the Judicial Redress Act, which gives European citizens the rights that are granted to U.S. citizens under the Privacy Act of 1974 and the right to sue the United States for unlawful disclosure of personal information . The official text of the Judicial Redress Act is available at *https://www.congress.gov/bill/114th-congress/house-bill/1428* (accessed 8 March 2016). See also European Court of Justice, C-362/14 (fn. 4), para 95.

(14) See European Court of Justice, C-362/14 (fn. 4), paras 63-66 and 102-104.

and the European DPAs (the Article 29 Working Party) will give their opinion on it in April (Article 29 Working Party, 2016). The Commission should take this opinion into account in the following adequacy decision.

Although, it is hard for the DPAs to express a negative opinion on the new agreement, due to the political and economic interests related to the data flows between the E.U. and U.S., they may express remarks that can affect the final decision of the European Commission.

Regarding the content of the new agreement, criticisms have been expressed by privacy associations, since the crucial aspects concerning the U.S. disproportionate data processing for surveillance purposes is still largely unsolved ([15]). In this sense, the agreement is a compromise that has a limited impact on the privacy threats enlightened by the ECJ in the Schrems case.

The agreement can be divided into two parts: 1) the Privacy Principles (Annex II); 2) the official representations and commitments provided by the U.S. Department of Commerce, the U.S. Government and the U.S. Department of Justice (Annexes I, III to VII).

The first part, on privacy principles and their enforcement offers a more detailed and higher protection than the Safe Harbor agreement. The risk-based approach, the principle of accountability of data gatherers, specific procedures for the complaints filed by E.U. data subjects and DPAs, and an active and *ex officio* monitoring of company compliance, are the main positive aspects of this new agreement. There are still grey zones (e.g. the opt-out model for non-sensitive data, the length of the complaint procedures), but the Privacy Shield reduces the gap between the U.S. and the E.U. standards of data protection.

Nevertheless, this is a provisional result, since the new E.U. regulation will introduce different changes and a more risk-oriented approach, which will probably recreate a substantial gap between the safeguards provided by the E.U. regulation and the protection provided by the Privacy Shield Framework Principles.

The second part of the agreement (Annexes I, III to VII), which primarily concerns the access and use of personal data transferred under the EU-U.S. Privacy Shield agreement by U.S. public authorities, is ne-

---

([15]) See the letter send by 27 privacy rights organizations to the Chairman of the Article 29 Working Party, the Chair of the Committee on Civil Liberties, Justice, and Home Affairs and the Ambassador and Permanent Representative of the Netherlands to the EU *https://edri.org/wp-content/uploads/2016/03/PrivacyShield_Letter_Coalition_-March2016.pdf.*

cessarily more vague. It is based on political assurances (e.g. "the U.S. government has assured the Commission that 'any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet'.") and future implementations (e.g. the Privacy Shield Ombudsperson ([16])). For these reasons and in absence of significant changes in the U.S. surveillance practices, many privacy associations are sceptical about the effective impact of this part of the new agreement.

3. – *Conclusions*

From a global perspective, the outcomes of the Schrems case and the re-definition of the U.E.-U.S. bilateral agreement on data transfer, which is still in progress, lead to a more thoughtful reflection on the future of the E.U. data protection model.

We should take into account the uncertainty about the effective application of this model, both within the E.U. borders (Kenneth et al., 2015) and outside (third countries regulations, standard clauses), and the political and economic reasons that make it weaker, as demonstrated by the compromise agreement with the U.S.

In this light, the main risk is the creation of a gap between the model as defined by regulations and various agreements and the effective provision of a high level of protection of fundamental rights and freedoms. The EU provisions on data flows, and on EU data sovereignty, seem to have mainly a declaratory nature, as demonstrated by the more formal than real safeguard of personal data existing in many EU countries and by the lack of control on the enforcement of the contractual solutions for trans-border data transfers.

This highlights the political nature of the E.U. data protection regulation, that can be understood only in the broader context of the multi-stakeholder dimension of global data protection, which involves different economic areas (US, EU, China, etc.) and different organizations (COE, APEC, OECD, UN). From this perspective, this legal wall built around European data, with its effects on international data flows, seems to be an instrument to reinforce the E.U. leadership in the drafting of a future global regulation for data protection, rather than a guarantee of an effective higher standard of protection.

([16]) According to the draft of the Privacy Shield agreement, the Ombudsperson will receive and respond to individual complaints regarding U.S. signals intelligence activities.

4. – *References*

Article 29 Working Party. 2016. *Statement of the Article 29 Working Party on the presentation by the European Commission of the EU-U.S. Privacy Shield*. Brussels. Available at *http: //ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160229-pressrel_publication_europeancommission_eu-us_privacy_shield.pdf* (accessed 14 March 2016).

Bamberger, K.A., and Mulligan, D.K. 2015. *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*. Cambridge, MA: MIT Press.

Chester, J. 2014. *CDD Files Complaint on U.S./EU Safe Harbor for Data Privacy at FTC/ Filing Reveals Failure of U.S. Agreement to Protect European Privacy*. Center for Digital Democracy. Available at *https: //www.democraticmedia.org/content/cdd-files-complaint-useu-safe-harbor-data-privacy-ftc-filing-reveals-failure-us-agreement*.

Connolly, C. 2013. *EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance. Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens"*. Strasbourg. Available at *http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf*.

European Commission. 2013. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU. Brussels. COM (2013)847 final. Available at *http: //ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf* (accessed 12 February 2016).

European Parliament. 2014. Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. Strasbourg. P7_TA (2014)0230. Available at *http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139* (accessed 12 February 2016).

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein. 2015. *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14*, para 4. Available at *https:// www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judg-*

ment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html (accessed 28 January 2016).

ALESSANDRO MANTELERO (*)

(*) This article is a revised version of a presentation given by the author at the BILETA 30th Annual Conference (University of Hertfordshire, Hatfield, April 12, 2016).