SECURING US-EU PERSONAL DATA FLOWS: A CRITICAL OUTLOOK ON THE RECENT AGREEMENTS"

No: 03

By: Giovanna Santori[1]

Email: giovanna.santori@yahoo.it

Abstract:

The development of data exchanges in the modern digital era, due to the relentless growth of the internet as a tool for worldwide commercial interactions, creates the issue of how to safeguard the enormous amount of personal information disseminated and which common standards must be set out for their treatment, in order for privacy to be ensured. The difference of approach in the privacy policy between EU and US may lead to conflicting regulations when it comes to handling cross-border data flows, both in the commercial and the police cooperation field. This article attempts to analyse the relation and the difference between the two systems, with a specific outlook on the agreements recently signed after the invalidation of the well known Safe Harbor Agreement by the European Court of Justice.

This paper was submitted as part of a competitive call for papers in the context of the 4th edition.

[1] Master (II level) on Constitutional and Criminal Law - University of "Roma Tre",LLB, University of Roma "Roma TRE"

Keywords: Data privacy – Privacy Shield – Safe Harbor

1. Data privacy in the EU and United States and the "adequacy requirement"

Europe and the United States have dramatically different approaches in addressing the right to privacy.

In Europe, the right to privacy is constitutionalised in several countries. Article 8 of European Convention of Human Rights formally grants every person the right to a private life[2]. In addition to overarching and well-constructed legislation, the right to protection of personal data is also enshrined in Article 8 of the European Charter of Fundamental Rights and Freedoms[3].

On the other hand, the US Constitution does not explicitly guarantee this right, which is partially regulated by some sectoral laws[4].

The reason for the difference lies, as it was asserted, in the concept of privacy as a value: privacy can be either conceived as an aspect of personal dignity – which refers to the right of the individual to protect his/her honor and reputation – or an aspect of liberty, which is the meaning that it holds in the American system, referring more to the freedom from the interference from the public powers[5].

---

[2] Convention for the protection of Human Rights and Fundamental Freedoms, 213 U.N.T.S. 222, *entered into force* Sept. 3, 1953, *as amended by* Protocols Nos 3, 5, 8, and 11 *which entered into force* on 21 September 1970, 20 December 1971, 1 January 1990, and 1 November 1998 *respectively*, at Art. 8: " *Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

[3]The Charter of Fundamental Rights and Freedoms of the European Union has become legally binding after the ratification of the Lisbon Treaty in 2009, O.J. (C306). Rat, Art. 8: "*Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."*; for a broad analysis, see European Parliament, *A comparison between EU and US data protection legislation for law enforcement, (2015), available at:* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

[4] The most significant is Privacy Act of 1974, 5 U.S.C. § 552a, enacted on 31 December 1974.

[5] James Q. WHITMAN, *The two western cultures of privacy: Dignity versus Liberty,* 113 Yale L.J. 1151 (2004).

Considering the amount of information exchanged, and the expansion of the digital services exportations, it goes without saying that a non-reconcilable divergence between the respective approaches could impact negatively on business relations. This is the reason why the need for a regulation that could link the opposite methods is essential for granting the legitimacy of the above mentioned operations, and to foster a more transparent market[6].

Within the European Union legal framework, Directive 95/46/EC[7] (Data Protection Directive, hereinafter DPD) regulates the flow of personal data, treated either by private or public organizations, from EU countries to third countries, on the basis of a previous scrutiny about the adequacy of the protection standards guaranteed by domestic laws, or international commitments, of that third country. This "adequacy test" is made by assessing if the use of data complies with the most significant DPD principles, which concern mainly the purpose of the collection, security and accuracy of the data, and the right of the individuals to access to them.

In case of a positive feedback, the transfer can take place without requesting any further safeguards.

In 2015, the European Parliament, the Council and the Commission reached an agreement on reform of the DPD, which had been proposed in 2012 by the Commission, with the intent to provide a more harmonised and modern legislation. The General Data Protection Regulation (GDPR, EU 2016/679[8]) came into force on 24 May 2016, replacing Directive 95/46/EC.

---

[6] Martin A WEISS and K. HARCHICK, *U.S.-EU data privacy: From Safe Harbor to Privacy Shield*, Congressional reasearch service (2016).

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Directive).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2. Protecting transatlantic data flows: the rise and fall of Safe Harbor Agreement

The direct consequence of the adequacy requirement was the implementation needed on third countries privacy regulative frameworks to be considered "adequate", according to the Directive guidelines. The activity that took place in this direction gave birth to three main instruments: Safe Harbor Agreement, Model Contractual Clauses and Binding Corporate Rules (BCRs).

Model Contractual Clauses are a form of standardised clauses that service providers (such as Microsoft) can use in their agreements with customers, to ensure that personal data transfers outside the EEA will be in compliance with EU Directive 95/46/EC requirements. On the other hand, Binding Corporate Rules ("BCRs") refer to a group of guidelines adopted by multinational groups of companies to regulate intra-group data transfers. To choose a general regulative tool may be preferable, under a cost-effective point of view, than signing a contractual clause every time there is a need for intra-group transfers.

In 2000, the US Department of Commerce and the European Commission issued the Safe Harbor Privacy Principles[9]. The newly released scheme established a streamlined process for US companies importing data from the EU, that can self-certify annually their compliance with the EU protection rules by declaring to abide by seven principles set out in the Safe Harbour framework: notice, choice, access, security, data integrity, and enforcement. Compliance with these standards was monitored by US federal agencies, like the Federal Trade Commission[10].

2.1. The Court's decision

[9] 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 Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (the "Safe Harbor adequacy decision").

[10] Over 4000 Us companies adhered to the Safe Harbor regime. The FTC has found violations of this international agreement in 2011 by Google, and 2012 by Facebook.

Safe Harbor has represented the reference legal framework for data operations involving privacy issues for more than a decade, until it failed the "suitability test" in front of the European Union top judicial body, that struck down the agreement in October 6, 2015[11].

The *casus belli* started with the complaint lodged in 2013 by an austrian citizen, Maximilian Schrems, before the the Irish Data Protection Commissioner. Schrems, a Facebook user since 2008, asked the Commission to investigate if the social media colossus effectively adhered to EU privacy protection standards in trasferring EU data, contracted by Facebook Ireland Ltd in the first place, to its servers in the United States. Schrems allegations were based on the information disclosure by Edward Snowden in 2013 ("Snowden leaks"), that put a shadow upon the lawfulness of American authorities operations in Europe, and also on the companies that were allegedly cooperating in such collection activities.

The Irish Comissioner initially rejected the complaint basing its decision on the fact that, participating to the Safe Harbor scheme, Facebook practices could be considered adequate. The case continued, as Schrems brought it to the High Court of Ireland, that decided to refer the case to the Court of Justice of the European Union. The issue was whether or not the adherence of a company to Safe Harbour granted a default legitimate position that the Data Protection Agency (DPA) was bound to accept with no interference, or did the DPA have power to practically assess, case by case, the conformity of a specific practice with fundamental rights (included in Charter of Fundamental Rights and Freedoms, and Directive 95/46/EC).

The CJEU had to judge if the Commission Decision, that determined the enactment of Safe Harbor in Europe, was an invalid European act.

The judges based the decision on two main grounds. Firstly, the Court observed that the derogatory regime contained in Safe Harbor scheme, which allowed companies to share data with

[11] *Maximillian Schrems v. Data Protection Commissioner*, C- 362/14 (Court of Justice of the European Union Oct. 2015); *See* also, Danielle KEHL, *European Court of Justice invalidates Key Part of U.S – E.U. Safe Harbor Agreement*, in Harvard Journal of Law & Technology.

U.S. authorities for security reasons, put the processing of information outside the scope of Safe Harbor provisions itself, particularly because transfers were not in conformity with the purpose for which they had been conducted. In other terms, U.S. authorities used those data way beyond what could have been strictly necessary to guarantee national security. Thus, such practices were obviously not able to grant standards of protection of fundamental rights equivalent to the EU ones.

Secondly, the impossibility for the DPAs to investigate, case by case, any privacy violation – because the alleged adherence of a U.S. company to Safe Harbor authomatically implied the legitimacy of its practices – was an unaccepatable limitation of such agencies' prerogatives for an effective oversight to prevent any misconduct.

Thus, the Court concluded that Safe Harbor Decision, as it was conceived, was invalid as irrespective of EU provisions.

3. Enhancing data privacy: The New "Privacy Shield" and "Umbrella Agreement"

The clamorous invalidation of Safe Harbor definitely signed a breakup point between the two privacy approaches from the opposite sides of the western world.

Even before the European Court decision, skeptical voices on the U.S. privacy policy had arisen within the international arena. In 2013, criticism became harsher after the unveiling of American National Security Agency's mass surveillance activities in Europe, and the suspicion that some important U.S. companies were involved in the collection operations carried out by governmental agencies[12].

Moreover, after the judgement, numerous concerns spread among privacy operators regarding the applicable regulation in cross-border data transfers, and the need for providing a new regulatory tool became a priority. Thus, EU and U.S. officials intensified the negotiations for a new framework that could replace the previous scheme and fill the gap left by the CJEU decision.

[12] In March 2014, for example, members of the European Parliament voted in favor of a resolution on the mass surveillance of E.U. citizens, which, among other things, called for the suspension of the Safe Harbor agreement.

The agreement arrived on Febraury 2, 2016, when the new Privacy Shield was announced[13]. The full text was released later that month.

On 12 July 2016, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield[14].

Privacy Shield sets out more strict obligations on companies handling european personal data, aimed to make the process more transparent, "in order to ensure an adequate level of protection", and enhance individual rights.

The most significant aspects of Privacy Shield framework can be summarised in seven key areas in which data protection standards have been strenghtened. The so called "Privacy principles are: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, and access, recourse, enforcement and liability"[15].

The core point of the agreement is the monitoring system established to verify the companies' compliance with the privacy principles; and the several redress options in case any individual wants to claim the misuse of his personal data. Individual complaints can be made: 1) directly to the company, which will have to give a reply within the following 45 days; 2) in addition, to an alternative dispute resolution body specifically designated; 3) to the national data protection authorities; 4) lastly, by submission to the "Privacy Shield Panel", an arbitration mechanism.

Privacy Shield includes also, for the first time, robust committments for U.S. public authorities to access to the data, which will be subject to strict safeguards and control mechanisms (as regulated in annexes to draft adequacy decisions), such as the Ombudsperson, an independent

[13] European Commission, "*EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*," press release, February 2, 2016.

[14] **Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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 (notified under document C(2016) 4176).**

[15] Annex II on Privacy Shield Adequacy Decision, full text available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

body tasked to handle complaints from EU citizens. On July 12, 2016 European Commission adopted the Privacy Shield Adequacy Decision.

The ongoing process for securing data flows between Europe and U.S. – especially for what concerns data breaches from public U.S. authorities – reached another significant step with the signature in June 2, 2016, of the "Umbrella Agreement", covering the treatment of information shared between EU-U.S. law enforcement authorities with the purpose to prevent and prosecute threats to collective security[16]. Through the framework, the legality of data transfers within the police cooperation activities will be guaranteed by providing strong safeguards such as regulation on data use – including retention time limitation, right to access and rectification – and the obligation to get previous consent before any data transfer activity.

Since the power of access of U.S. authorities was a sticking point, the adoption of the agreement was conditioned upon the approval of a law granting EU citizens, regardless if they reside in the United States, a judicial redress right. The law was enacted on February 24, 2016, when President Barack Obama signed the Judicial Redress Act, granting the above mentioned redress rights. On december 1, 2016, the European Parliament approved the Umbrella Agreement which can now be finalised and enacted.

4. Conclusion. The ongoing battle to balance privacy and security

The above listed agreements undoubtedly witness the effort to achieve a common privacy framework more compliant to european standards. Although there is still room for improvement (EU Parliament and Art. 29 Working Party outlined some deficiences in the renewed mechanisms[17]), they represent a progress in the fulfilment of a safer global data exchange, and are

[16] Council Decision (EU) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.

[17] See Article 29 Working Party, *"Statement on the decision of the European Commission on the EU-U.S. Privacy Shield*", July 26, 2016, http://ec.europa.eu/justice/data-protection/article-29/press-material/pressrelease/art29_press_material/2016/20160726_wp29_wp_statement_eu_us _privacy_shield_en.pdf, where the Group states that <<*The WP29 welcomes the improvements brought by the Privacy Shield mechanism [...] However, a number of these concerns remain regarding both the commercial aspects and the access by U.S. public authorities to data transferred from the EU* >>.

definitely paving the way for further lawmaking activities that seek to abide with the european protection levels, according to whom the right to privacy is a non-negotiable human right.

Considering that 1995 Data Protection Directive provisions stated that personal information could be transferred to a third country only if "an adequate level of protection" was granted, the efforts to overcome EU concerns over U.S. privacy policy clearly demonstrates the mutual intent to allow data exchange, in the awareness of its importance for the economic growth. Only in this way a "privacy collision", as it was called, could be averted[18].

According to what indicated above, the biggest obstacle that could hinder the strengthening of U.S.-EU relations and the mutual adherence to a common value of right to privacy is the security need, that seemed many times a prevailing interest in the american perspective.

In the *"Schrems case"*, the CJEU reasoned that, as the American system basically enabled organizations to disregard some of Safe Harbor rules when a security need may come up, a genuine application of the principles couldn't be considered that assured. Thus, whether or not Safe Harbor provisions were adequate, allowing an interference in the individual rights without defining any satisfactory limitation was not going to be acceptable.

The struggle to balance privacy with security is a well known issue in the european legal system. It is emblematic that in *"Schrems case"*, the Court recalled a principle expressed in another important decision, the *Digital Rights Ireland* case (C-293/12 and C-594/12)[19], in which the Court invalidated the Data Retention Directive 2006/24/CE[20] on the basis that the data collection

---

[18] Paul M. SCHWARTZ, "*The EU-US privacy collision: a turn to institutions and procedures",* 126 HARVARD LAW REV I966, (2013).

[19] *Digital Rights Ireland and Seitlinger v Minister for Communications, Marine and Natural Resources* (C-293/12 and C-594/12) [2014] E.C.R. I-238; [2014] 2 All E.R. (Comm) 1.

[20] Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (Data Retention Directive) [2006] OJ L105/54.

procedures, carried out in the light of that regulation, were not proportionate with the purpose of preventing crimes and international security threats[21]. According to Art. 52.(1) of the Charter of Fundamental Rights, limitations to the excercise of a principle recognised in the Charter itself *<<may be made only if they are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others>>*. It is exactly in the proportionality requirement, expressed in article 8 ECHR as what is "*necessary in a democratic society*"[22], that lies the key criterion to handling privacy-security conflicts: any legal measure that allows an inteference in the private life of citizens should always be proportionate and never go beyond what is strictly necessary according to the intent declared.

In conclusion, primacy of security needs shall never disregard the core essence of a fundamental right to be legitimate, and this is what Privacy Shield and Umbrella Agreement, as well as other future data retention schemes or national legislation, will have to pursue.

[21] *Digital Rights Ireland* (C-293/12) at [125]: *<<In conclusion, The Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples, and DNA profiles of persons suspected but not convicted of offences, as applied in the case of present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation>>*.

[22] *Supra* note 1.