derecom

ISSN: 1988-2629. Nº. 19. Nueva Época. Septiembre 2015-Febrero 2016

Cómo citar este texto:
Zwolinska, M. (2015). International transfers of personal data. Towards a global consensus on data protection standards. Derecom, 19, 165-181. http://www.derecom.com/derecom/

INTERNATIONAL TRANSFERS OF PERSONAL DATA. TOWARDS A GLOBAL CONSENSUS ON DATA PROTECTION STANDARDS

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES. HACIA UN CONSENSO GLOBAL EN NIVELES DE PROTECCIÓN DE DATOS

© Monika Zwolinska
University of Nice-Sophia (Francia)
m.zwolinska@yahoo.com

Summary

We present in this contribution the disparities that exist between the European and American approaches to protecting personal data. Those two legal traditions are very different from each other. That is a barrier to establishing secure and effective systems of transferring personal data between the two continents. Elaborating a common ground for those transfers is an essential step in developing commercial cooperation. One of the key criticisms of the current international regime is its failure to meet needs of today's global business environment. The question we will ask is whether it is possible to reach an agreement on the strategic issue of cross-border data transfers in the light of the American large conception of freedom to do business and to keep the governmental intervention as rare as possible, on the one hand, and the European high standards and adequacy requirements applicable to data confidentiality, security and integrity.

Resumen

Esta colaboración presenta las diferencias que existen entre el enfoque europeo y el norteamericano en cuanto a la protección de datos personales. Esas dos tradiciones legales son muy diferentes entre sí. Esto es una barrera a la hora de establecer un sistema seguro y efectivo de transferencia de datos personales entre los dos continentes. Elaborar una zona de encuentro para esas transferencias es un

paso esencial en el desarrollo de la cooperación comercial. Una de las críticas clave del régimen internacional actual es el fracaso en cuanto a la satisfacción de las necesidades del entorno empresarial global actual. Lo que nos preguntaremos es si es posible alcanzar un acuerdo sobre la cuestión estratégica de la transferencia internacional de datos a la luz de la amplia visión norteamericana de hacer negocios y mantener la intervención gubernamental tan alejada como sea posible, por un lado, y a la luz de los elevados exigencias y estándares mínimos aplicables a la confidencialidad de los datos, seguridad e integridad.

Key words: Personal data, Cross-border data transfers

Palabras clave: Datos personales, transferencias internacionales de datos

INTERNATIONAL TRANSFERS OF PERSONAL DATA. TOWARDS A GLOBAL CONSENSUS ON DATA PROTECTION STANDARDS

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES. HACIA UN CONSENSO GLOBAL EN NIVELES DE PROTECCIÓN DE DATOS

© Monika Zwolinska
University of Nice-Sophia (Francia)
m.zwolinska@yahoo.com

Summary

We present in this contribution the disparities that exist between the European and American approaches to protecting personal data. Those two legal traditions are very different from each other. That is a barrier to establishing secure and effective systems of transferring personal data between the two continents. Elaborating a common ground for those transfers is an essential step in developing commercial cooperation. One of the key criticisms of the current international regime is its failure to meet needs of today's global business environment. The question we will ask is whether it is possible to reach an agreement on the strategic issue of cross-border data transfers in the light of the American large conception of freedom to do business and to keep the governmental intervention as rare as possible, on the one hand, and the European high standards and adequacy requirements applicable to data confidentiality, security and integrity.

Resumen

Esta colaboración presenta las diferencias que existen entre el enfoque europeo y el norteamericano en cuanto a la protección de datos personales. Esas dos tradiciones legales son muy diferentes entre sí. Esto es una barrera a la hora de establecer un sistema seguro y efectivo de transferencia de datos personales entre los dos continentes. Elaborar una zona de encuentro para esas transferencias es un paso esencial en el desarrollo de la cooperación comercial. Una de las críticas clave del régimen internacional actual es el fracaso en cuanto a la satisfacción de las necesidades del entorno empresarial global actual. Lo que nos preguntaremos es si es posible alcanzar un acuerdo sobre la cuestión estratégica de la transferencia internacional de datos a la luz de la amplia visión norteamericana de hacer negocios y mantener la intervención gubernamental tan alejada como sea posible, por un lado, y a la luz de los elevados exigencias y estándares mínimos aplicables a la confidencialidad de los datos, seguridad e integridad.

Key words: Personal data, Cross-border data transfers

Palabras clave: Datos personales, transferencias internacionales de datos

1.Introduction

Nowadays, businesses increasingly operate on an international basis both internally, within global group structures, and externally, with networks of customers and suppliers. With the economic globalization and explosion of digital industry, single data processors have turned into multitasking processing actors charged with data processing, storing, and transferring in ways that are much easier, quicker and cheaper than ever before (Birnhack, 2008).

However, as such technologies as cloud computing and Big Data develop faster than we can imagine, a new phenomenon has become a particularly important issue. Personal information about individuals is, indeed, being processed overseas, frequently without the explicit knowledge or consent of those individuals. The protection of this information is ambivalent, based on the fact that they are dematerialized. Yet, personal data presents a real monetary value as well for individuals as for businesses and therefore it has become a tangible asset. The security of such data is, in this context, a complex and still unexploited legal area. It raises questions of who may have access to it and for what purposes and what rights the individual may have to object.

Today, the main barriers to safe and commercially-friendly international data transfers are linked to the fact that compliance with foreign data privacy laws is extremely difficult. Each region (or even country) establishes its own rules and the differences are significant. For the purpose of this paper, we will focus on the United States of America (USA, from now on) and on the European Union (EU, from now on) rules, though one must keep in mind that the Asian system is also increasing its significance with its digital business constant growth.

In the first part of this paper, we shall define fundamental concepts of international data transfers in the EU and in the USA systems and discuss their main differences which stand in the way of the free flow of personal information. In the second part, several same or similar principles in both of those systems shall be determined, leading to the conclusion that some common ground is possible to achieve in order to obtain a consensus on international standard for personal data transfers.

2.Major disparities in the EU and in the US personal data approaches

Europe has a long history of data protection and has traditionally been seen as having a higher standard in this legal area than the rest of the world.

A) Differences in fundamental concepts of personal data

While a new regulation proposal on protection of personal data is still under examination (the "General Data Protection Regulation"),[1] the European Union 95/46/CE Directive[2] remains the fundamental text establishing rules for data processing and transfers for now. According to this Directive, an international data transfer shall be defined as a transfer of personal data to a third country (which is any country outside of the European Economic Area, EEA, from now on) and reaching a recipient data importer in a third country. Therefore, this kind of transfer occurs whenever data leaves the territory of EU, Iceland, Liechtenstein and Norway.

From the perspective of the United States, it is even simpler because an international data transfer is a transfer that goes beyond any of the American States.

The main principle of the 95/46/CE Directive is that it establishes the free flow of data within Member States while at the same time it prohibits transfers outside the EEA, unless the third country which is the data recipient provides for an "*adequate level of protection*". Since adequate protection does not automatically mean "equivalent one", the section 25 of the Directive introduces and "*adequacy assessment*". This assessment shall be led in light of all circumstances evolving around the transfer, through a non-exclusive list of criteria pertaining to the content of the rules and the mechanisms in place for ensuring that data protection principles are applied. Both of them may derive from legislation and industry self-regulation. For instance, the transfer of a list of internal telephone extensions to overseas subsidiaries of a multinational company would not be considered to be high risk as it is unlikely that a data subject would suffer significant damage if his business telephone number was obtained by an unauthorized recipient. However, if a data exporting controller is proposing a transfer of sensitive personal data (e.g. health records), the level of protection required for the data (and the rights of the data subjects) will clearly be higher. Moreover, some purposes for which data are processed will carry greater risks to the rights of the individuals than others. For example, if the data are to be processed for internal company or group purposes only (such as the internal company telephone list as described above), the transfer of such data may involve less risk to the rights of the data subjects than if the data transferred is to be distributed more widely (e.g. customer contact details to be used in marketing or on an internet site).

To avoid a case-by-case adequacy examination, the European Commission has issued several decisions putting some countries on a "white list" of those that, since they present sufficient level of protection, may receive data transfers with no additional restrictions. This list includes Argentina, Canada, Guernsey, Jersey, Isle of Man and Switzerland – but not the United States of America. These adequacy decisions apply to personal data in a general manner, though they do not cover data exchanges in the law enforcement sector. For special arrangements concerning exchanges of data in this field, the PNR (Passenger Name Record)[3] and the TFTP (Terrorist Finance Tracking Programme)[4] agreements must be applied.

As for the definition of what is actually being the object of protection in data transfers, both systems have a different answer. For Europeans, those are "personal data" which means

> "*any information relating to an identified or an identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural and social identity*" (article 2(a) of the Directive, article4 (1) of the draft regulation).

In short, any information that can be used to identify an individual constitutes personal data. For example, a list of customer names and addresses will count as personal data, as may a database of customer email addresses count too. Therefore, the European definition is very broad and, as a consequence, most businesses will be directly concerned by it as they detain information about their clients and suppliers.

Yet in the United States, even though a definition of personal data similar to the European one exists, the central notion connected to the international transfers issue is "privacy". Indeed, the main text that applies in this domain is the Privacy Act of 1974. Much wider in its scope, it is usually

interpreted as "*the right of individuals and/or organizations to decide which information about them may be transferred to other parties*" (Hew Report, 1973). The right to privacy as protected by the American constitution has gained a foothold in the landmark decision Griswold v. Connecticut in 1965.[5]

The concept of privacy is also very close to the one of "informational privacy", which refers to one's "*control over personal information*" (Solove, Schwartz, 2009). Therefore, under the American law, privacy shall be considered as the right of people to lead their lives in a way that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbor's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera. It is also a right of the people to be free from unwarranted electronic surveillance. For instance, the Federal Communications Commission has issued regulations[6] restricting companies from certain forms of telephone solicitation, which has evolved into common annoyance in American households. Under these regulations, a company is not allowed to start a telephone call by using an automatic dialling system or artificial or prerecorded voice without prior consent of the person called.

Thus, as opposed to the European system, the notion of "*personally identifiable information*" is not commonly used in the USA legal texts, although it is defined by the American Code[7] and is employed by some recent legislation covering the subject of identity theft[8], for example. Yet, one must continue to distinguish between the still commonly used "privacy" and "data protection". In practice, there may be occasions where the right to data protection is applicable on a given set of data, but the processing of this data at the same time does not infringe the given individual's right to privacy (De Hert, Gutwirth, 2009). All in all, it is often highlighted that American privacy laws are considerably weaker than the European ones, with only one Consumer Privacy Bill of Rights applied since February 2012 – but simply based upon voluntary codes of conduct (Epic, 2013).

The gap between the two conceptions is that where the EU law protects personal data as inalienable human rights, US legislation considers its protections as part of preserving purely economic value of this data, as it is an alienable commodity subject to business transactions. This is a result of more general philosophy where while in the EU an individual is considered as a subject of fundamental human rights who needs protection in order not to become victim of a potential abuse by the most powerful, in the USA, an individual is first of all considered as a consumer who can seek his rights´protection by himself through the judicial system using legal tools provided by the State (Marcinkowski, 2013).

It is therefore argued that harmonizing two systems which aim at protecting two separate concepts (one of them being much wider in scope and much more practical than the other) may not be even possible.

B) Differences in rule-making and rule-applying solutions

Generally speaking, the American legal system does not provide for an adequate degree of personal data protection, from the EU legal perspective. As for practicalities, one of the critical reasons for this conflict of adequacy is the lack of uniformity of the criteria applied by the EU in the adequacy text and their unclear hierarchy. For example, the amended Federal Data Protection Act of Germany is more stringent than the EU's Data Protection Directive. The German data protection authorities have certain reservations against the Safe Harbor Principles as, according to their assessment, these principles do not offer data protection standards that are common with those of the European Union[9]. Also, a recent PUPIE Report from 2013 clearly proves that the harmonization of European laws is still a work-in-progress, with a number of areas concerning data protection that need to receive more clarity.[10] It has,

therefore, been considered for several years that "*differences in the way that each Member State implements the law have led to inconsistencies, which create complexity, legal uncertainty and administrative costs. This affects the trust and confidence of individuals and the competitiveness of the EU economy*."[11]

But more theoretically, and more fundamentally, this is the conflict between the European Statutory Law and the American Common Law approaches. Several conclusions derive from this two pillar system.

On the one hand, the European approach is that data should be protected by compiling all norms regulating the entire area of data protection into one legal act functioning as a sort of a "constitution" for the entire field (both in public and private sectors), with clear legal hierarchy. On the other hand, Americans prefer a system of regulatory fragmentation where in absence of a unique fundamental legal act regulating the entire area of informational privacy (the exception being the Privacy Act applicable at a federal level, though only to the public sector[12]), several legal acts cover each a specific sector. Thus, State and Federal legislation regulates the circumstances under which information from financial, educational and government records may be revealed. Federal laws strictly limit the use of electronic surveillance in both public and private sectors, too. The Health Insurance Portability Act of 1998 (HIPAA) is a prime example of data protection implemented in only one field (health care). As one author explained, under the USA privacy protection approach, "*regulation is perceived to intrude on the commitment to freedom from government interference in information flows. As a result, law emphasizes regulation of the market process rather than the substantive contours of information privacy*".[13]

Moreover, whereas European approach is based on an administrative method where the elimination of imbalance is mainly achieved through the involvement and exercise of power by the State (by intermediate of personal data protection bodies such as ICO, CNIL or APD), in the United States, the emphasis is on private law mechanisms, including self-regulation and self-certification, working along with a judicial oversight (and with no specific body designated in particular to protect data).

In this matter, some opinions are that the EU directives create unnecessary compliance burdens on companies (Kamarinou, 2013). Being inflexible and giving the State excessive discretionary powers, it may limit innovations in the economy. There is an issue as to whether the legislation has been overtaken by commercial and technological advances and whether the overseas transfer requirements in fact place unreasonable and unrealistic demands on companies and organizations that transfer data overseas (such as the requirement to notify any breach in data protection within 24 hours following its discovery). In addition to that, it has been argued that if facing harsh compliance requirements, business is more likely to focus on technical compliance with data protection rules than on the outcomes and the protection of the consumer. Nevertheless, this European pattern presents some virtues. It is actually quite transparent and homogeneous, which makes it easier to navigate for individuals.

As for the USA approach, it is often praised for its flexibility and for leaving the power of initiative and freedom to individuals. But it is far from being perfect and some of its backlashes are: potential passiveness toward data violations (as opposed to increasing liability under EU law in such cases), as well as difficulties in navigation between different legal texts. Therefore, difficulties in everyday application of the law are very likely to arise. Finally, what is the biggest disadvantage of the

American system is that because the self-regulation reflects primarily business needs and interests, individuals may suffer from protection standards being established to their disadvantage (Rotenberg, 2001).

The facts show that EU-USA cooperation on such sensitive issue as personal data protection is not an easy task. In 2006, a High Level Contact Group within a police and justice area has been created on a common initiative. Its role was to become an advisory group to discuss data protection in the context of fighting terrorism and to facilitate bilateral cooperation in at least one of the fields: the law enforcement. But the group's Report in 2008[14] was criticized in Europe for lacking transparency during the negotiations procedure (Wright, De Hert, Gutwirth, 2011).

America's fight against terrorism and its constant search for strengthening national defence is actually one of the main examples of how personal data do not receive so much protection in the USA as they do in Europe. Thus, the USA Patriot Act, 2001[15], introduced a plethora of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the USA. However, this act does not provide for a substantial system of checks and balances that traditionally safeguarded civil liberties in the face of such legislations. As a result, law enforcement authorities and intelligence agencies may monitor private communications and access personal information, especially those concerning non-USA citizens. It therefore lacks appropriate protection of individual liberty, including regulations on interception of information transmitted over means of electronic communications including cloud computing. This view is more and more shared by USA citizens. For instance, the Pew Research Centre has recently published a new privacy poll on Americans' Views About Data Collection and Security (Pew Research Centre, 2015). According to this survey, 74% of Americans believe control over personal information is "very important," yet only 9% believe they have such control.

To sum it up, the Transatlantic debate is one between precise, explicit and specific public law regulations in Europe and flexible, pro-market, self-regulated, segmented, sectorial regulation in the United States (Regan, 1999). But even though those two systems differ in the way they create laws, as well as in the way they apply them, common language between those two approaches remains a necessity and some common grounds may be identified in order to elaborate a harmonized cooperation.

3.What common grounds exist and how can they be basis for elaborating an international standard

A) Similarities between the American and the European systems

There exist some common grounds between the American and European systems on how data transfers should be conducted. This is demonstrated by the fact that both parties managed to elaborate the co-called EU-US Safe Harbour Privacy Principles which allow American companies to adhere to a specifically construed program which allows them to issue and receive personal data transfers from Europe without additional restrictions. Almost 3,500 organizations across a broad range of industries are Safe Harbour-certified (McBride, Sotto, Treacy, 2013). Moreover, a transatlantic agreement has been achieved for the transfer of Air Passenger Name Records to the USA Bureau of Customs and Border Protection (see the above-mentioned PNR Agreement). European Court of Justice is in charge of controlling its application, as well as European Commission's decisions on adequate protection concerning PNR data. This gave birth, for instance, to situations where transfers of PNR of air passengers from the EU to the US Bureau of Customs and Border Protection were considered to be illegal and had to be canceled.[16] In the

C-318/04 case, the Court held that the Commission's decision was wrongly based on the 95/46/EC Directive because the processing of the data put at the disposal of the United States information concerning public security and the activities of the State in relation to criminal law and the fight against terrorism. Yet, processing data for such purposes is outside the scope of the protection afforded by the Directive according to its article 3 §. The judge argued that the collection and transfer of the data by the airlines was required by law for reasons of public security unrelated to their provision of transport services to passengers.

Moreover, even though Europeans tend to protect "personal data", whereas Americans are more concerned with "privacy", it can be found that the core values the both systems are tending to enshrine are very similar, if not identical (Marcinkowski, 2013). In fact, neither the European nor the American aim to protect data or privacy shall be considered as a goal in itself but rather as a way to preserve fundamental values in a democratic society. And those fundamental values are, indeed, common to both social and legal cultures: freedom from unlawful or unreasonable government interference in individual's life, freedom of interference of any other third parties, freedom of expression, freedom of information, self-determination, etc.

Therefore, despite their discrepancies addressed before, the terms of "personal information" and "privacy" are likely to present similar characteristics depending especially on how the second of them is interpreted. Indeed, one should keep in mind that the meaning "privacy" may change according to its legal context. In constitutional law, privacy means the right to make certain fundamental decisions concerning deeply personal matters free from government coercion, intimidation or regulation. In this sense, it must be associated with interests in autonomy, dignity and self-determination. Under the common law, it should be interpreted as a right to be left alone and therefore associates with seclusion. Finally, under statutory law, it usually means the right to prevent the non-consensual disclosure of sensitive, confidential or discrediting information. In this last context, it is associated with secrecy. As a consequence, both EU and USA systems share the same axiological foundations as long as all those elements: informational self-determination, right to be left alone and preservation of confidentiality of one's own information, that may be considered as common goals in both types of legislation.

Additionally, as such, EU rules are in accordance with the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980. Since these guidelines have also been recognized by the US, it is natural that both European and American laws, when it comes to making rules on personal data transfers, be inspired by the same core of principles: collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle or accountability principle.

Several basic statements in terms of individuals' rights over their data derive from this set of principles. For example, any system that would inspire itself by those principles shall prohibit any personal data record-keeping files whose very existence is secret. Also, every single individual must always have a way to find out what information about him or her is in record and how it is used. He or she shall moreover be able to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent. He or she should finally be able to correct and amend a record of identifiable information about him or her.

There also is basic consensus on the fact that any organization creating, maintaining, using or disseminating records of personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. Some universal fair information

practices shall, therefore, be possible to emerge. Those practices can be inspired by Fair Information Practice Principles elaborated in the USA in 1973[17] which include such principles as transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security or accountability and auditing. In the USA, those principles are most of all embodied in the Privacy Act and the Fair Credit Reporting Act, but also in many sectorial legislations like the Family Educational Rights and Privacy Act (FERPA).[18] In this last text, for instance, the legislator has imposed a requirement which regulates the "*educational records*" of a university, carefully defining the records that are within its scope and regulating the relationship between university and student, rather than imposing rules on the disclosure of grades under all circumstances. More recently, the data brokers[19] industry has been put under scrutiny from the Federal Trade Commission and the Senate Commerce Committee. As a result, a new initiative has been launched. Under the title "Reclaim Your Name" it is designed to promote more transparency in the data broker industry and give consumers greater control over their individual data (Committee on Commerce, Science and Transportation, 2013). Following this review, in March 2015, a bill entitled "The Data Broker Accountability and Transparency Act" has been released by Senators (Dwork, Mulligan, 2013).

In the EU, the Practice Principles have served as inspiration when drafting the 1995 Directive. Also, with the upcoming regulation, a new divergence point is increasing its significance: the very controversial right to be forgotten incorporated in article 17. And although it is highly criticized for its technical infeasibility, as well as incompatibility with the functioning of the digital economy – and has indeed become one of the major bones of contention between Europeans and Americans, it is still founded on the same principle which has already been recognized by the Fair Credit Reporting Act that gives consumers the ability to correct false information in their credit reports and it places limits on the ability of credit reporting agencies to disclose old information about consumers, like criminal records or lawsuits older than seven years)

All of those fundamental principles are the intellectual basis for elaborating rules on both sides of the Atlantic. Since this basis is acceptable for both systems, there probably is a way to make them work together as a whole, instead of maintaining a somewhat chaotic patchwork of legal solutions constructed on a limited, *ad hoc* basis (Safe Harbour Framework for Commercial Data Exchanges, specialized agreements for PNR exchanges, SWIFT exchanges in the banking industry, law enforcement data exchanges, etc.)

B) In search of a common standard for international data transfers

It is generally argued that international consensus on the issue of personal data transfers might provide stability and level the competition among data processors (Gunasekara, 2009). International actors look forward to some level of harmonization, especially in the light of recent widespread concern about the USA government's covert surveillance programs which has raised doubts concerning the "safety" of the Safe Harbour. In June 2013, there were reports of the USA and the EU authorities intercepting and accessing the electronic communications of EU citizens on an extensive scale, in part, pursuant to the American PRISM program. Following these reports, in July 2013, the European Parliament called on the European Commission to review the Safe Harbour (McBride, Sotto, Treacy, 2013).

This uncertainty may, in practice, result in important legal conflicts, such as the one that has presented itself before the Court of Justice of the European Union on 24 March 2015[20]. In this case, an Austrian national has challenged the legality of a decision by the Irish Data Protection Commissioner of not investigating his claims relating to data transfers to the USA by Facebook, based on the company's Safe Harbour membership. The person argued that the Safe Harbour does not entirely warrant adequate

data protection because of widespread data access by US intelligence services. In brief, the questions asked were whether the national data protection authorities are absolutely bound by a Commission adequacy decision with regard to data transfers to third countries, or whether they may conduct their own investigations into the adequacy of data protection in light of articles 7, 8, and 47 of the EU Charter of Fundamental Rights. The final decision has not yet been issued.

Yet, globally speaking, current European data protection policy is to strive for the adoption of worldwide binding standards for personal data transfers inspired by the international standards elaborated at the 2009 Data Protection Conference in Madrid, and supporting the effort of the Council of Europe to promote the adhesion of third countries to the Convention 108 and its Additional Protocol. Furthermore, the European Draft Regulation on Personal Data is the first step towards the American system. Aiming at a greater degree of flexibility for all parties involved, it introduces the accountability principle (articles 22, 42, 43) by laying down for processors the responsibilities, the compliance tools and their possible liabilities under the data protection corporate clauses, while maintaining the general adequacy system assessed by the Commission (Kamarinou, 2013). On the top of that, it legally recognizes the concept of Binding Corporate Rules.

Also, the Draft Regulation simplifies the approval process, extends the concept to processors and a "*group of undertakings*" and admits some new derogations to the adequacy requirements (article 44). This is, for example, the case where the transfer is authorized by a previous consent of the data subject, given in an "*unambiguous manner*" (article 26.1(a)); where the transfer is necessary for the performance of a contract between the data subject and the controller; where the transfer is necessary for important grounds of public interest; or where the transfer is necessary in order to protect the vital interests of the data subject or of another person.

It results from the above that the door is continuously opening to free flowing of European citizens' data. Such evolution may partly be explained by some strong lobbying efforts of the American giant technological companies such as Google, Yahoo, Microsoft or Amazon that managed to play a remarkable role in negotiations. As a result, the conflict between the European and the American approach rather turns to be one of businesses pushing towards lighter regulation for the sake of supporting innovation, on the one hand, and citizens advocating a debate on the rise of online profiling and erosion of informational self-determination.

Moreover, the EU and US respectively systemic solutions are gradually evolving and the tools of both legal cultures start to blend with each other (Marcinskowski, 2013). This is reflected, for example, by the pattern Standard Contractual Clauses or Binding Corporate Rules which are EU measures designated to allow transfer of personal data from the EU to other countries. They provide for varying levels of involvement of administrative bodies. Those measures are in fact based on contractual schemes and adapted to modern business schemes, which are qualities historically characteristic to the American approach. Today, they play a major role in data exchanges between the EU and the USA outside of the European Commission adequacy test. Globally speaking, a turn in personal data governance can be observed for several years, leading to the proliferation of soft law (codes of practice, ISO standards, trustmarks, etc.) as an alternative to formal regulation, as well as to the introduction of data privacy norms into regulative texts of a different subject matter (for instance, in consumer protection laws, employment laws, spam laws, etc.). Simultaneously, the American Federal Trade Commission is becoming more active in regulating data protection, therefore increasing the degree of protectionism and bringing the American pattern closer to the European one.

Furthermore, since March 2011, the European Union has been negotiating with the United States government an International Framework Agreement (called "Data Protection Umbrella Agreement") in order to protect personal data transferred between the EU and the USA for law enforcement purposes. This includes cases in which personal data is sent from the EU to the USA for the prevention, detection, investigation and prosecution of criminal offences, including terrorism. Some of the fundamental principles included are: non-discrimination and maintaining the quality, integrity and security of data.

Next step in Transatlantic rules harmonization could be establishing an independent body devoted to personal data protection. The role of such institution would be to oversee and ensure that government agencies conform to the "right to privacy" legislations all over the world (De hert, Papakonstantinou, 2013). Such a single, uniform regulatory tool would need to overhaul divergent European and American data protection schemes, reevaluating established approaches and procedures. In order to do that, the setting of a new international data privacy tool is not absolute necessity. Instead, an international set of rules already adopted in the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files could be used, for instance, in its adapted and/or expanded version.

Conclusion

In an ideal world, global framework balancing interests of data subjects and data controllers could be feasible if only cultural, historical and legal differences between national sovereignties could be compromised and all the relevant major stakeholders could agree on the form, scope and basic standards of a global instrument.

In reality, one shall not hope for any radical change in upcoming years and as each of the regulators – EU and USA – consider their approach to prevail over the other, no unique, fixed, common legal framework should be expected to arise. Even the new EU personal data regulation, although it truly is a step toward uniformity, does not introduce a "radical rethinking" on international transfers, that might be considered a change the data regulators had previously called for.

The consequences of this disharmonized system may be essential as, for example, the right of effective judicial redress is still not properly granted by the Americans to EU citizens not resident in the USA.

What we should expect, however, is for public authorities to elaborate a common ground where different international public measures could come along with instruments of self-regulation and co-regulation in order to make the international data transfers rules interoperable, for the sake of individuals being able to decide themselves, with the help of State's safeguards, how far they want the moderns business to interfere with their personal lives.

Indeed, questions relating to privacy in digital age are essential to the functioning of the international economy as a whole. As results from recent studies (MEF, 2015), trust – which is directly linked with people believing that personal data transfers do not interfere with their privacy and their dignity - remains the largest single obstacle to growth in the digital and mobile content and commerce industry. Furthermore, data transfers cause much concern within organizations operating internationally and within Europe, especially with the increasing powers of regulators to levy financial penalties. This is, for example, the case of the new General Data Protection Regulation which states, in its clause 79, that a fine up to 100 000 000 EUR, or up to 5% of the annual worldwide turnover in the case of an enterprise, applies in case of a breach of these new data privacy regulations.

Whatever happens with the European Draft Regulation (since there still is a risk it would not be adopted as such and it would rather turn into a new, less precise Directive or even be abandoned), there is no coming back from the fact that both systems are mutually becoming more and more alike. Europeans start to understand that data flows are crucial for contemporary business and that, while they continue preserving fundamental rights of individuals to keep their own data under their control, they also have in mind not to put unnecessary obstacles in European businesses' way.

As for Americans, much more liberal about protecting privacy, they have suffered several cyberattacks in last few years (Sony Pictures, eBay, JP Morgan Chase, AOL, etc.) and they start to realize that better protection on individuals' data is going to be one of the biggest challenges of upcoming policies. The evolution has already begun, with, for example, recent Obama's law proposal on the protection of consumers´ data (Data Security and Breach Notification Act, March 12th 2015) – directly inspired by European's obligation to notify data breaches.

What one must keep in mind in the context of this evolution is that before new legal measures are adopted and new information technologies introduced, the concept of Privacy by Design must be put forward – as it has been by article 23 of the EU Draft Regulation (Kuner, 2009). This implies that a proper and sustainable impact assessment is taken into account so that any potential interference with privacy does not outweigh the genuine added value of the intended legal measure or information technology.

---

[1] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), C7-0025/12, see : http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

[2] 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 on the free movement of such data , OJ L 281, 23.11.1995, p. 31–50, see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[3] The EU has signed bilateral Passenger Name Record (PNR) Agreements with the United States of America, Canada and Australia. PNR data is information provided by passengers during the reservation and booking of tickets and when checking in on flights, as well as collected by air carriers for their own commercial purposes. PNR data can be used by law enforcement authorities to fight serious crime and terrorism.

[4] The EU has also signed a bilateral agreement with the USA - the Terrorist Finance Tracking Programme (TFTP) - regulating the transfer of financial messaging data.

[5] 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965). In this decision, the Supreme Court struck down a State Statute forbidding married adults from using birth control measures because the statute violated the sanctity of the marital bedroom. Acknowledging that the Constitution does not mention the word "privacy" anywhere in its text, the Court held that a general right to privacy may be inferred from the express language of the First, Third, Fourth, Fifth and Fourteenth Amendments, as well as from the interests protected by them.

[6] 47 C.F.R. § 64.1200

[7] 1028(d)(7) of title 18, United States Code: the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—
(A)name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(C) unique electronic identification number, address, or routing code; or
(D) telecommunication identifying information or access device (as defined in section 1029 (e)).

[8] S. 1897 (113th): Personal Data Privacy and Security Act of 2014.

[9] For instance, in order to send data to Germany, the data exporter cannot simply rely on a statement by the data importer that it is Safe Harbour certified, the data exporter rather has to check whether the Safe Harbour Principles are actually adhered to and ensure that the certification is still valid. The data importer must show the data exporter proof of the certification, even if it appears on the Safe Harbour list of the USA Federal Trade Commission. Furthermore, the data importer must prove that it is complying with the obligation to notify data subjects about the processing of their personal data and indicate how it fulfils this obligation. The data exporter must keep a record of these checks on the data importer and make this record available to the data protection authorities on request. To avoid any doubt, the German data protection authorities recommend the use of EU standard contractual clauses rather than relying on Safe Harbour.

[10] "Recommendation R (87) 15 - Twenty-five years down the line", a Report by Professor Joseph A. CANNATACI and Dr. Mireille M. CARUANA, first submitted on 12 November 2011 with a revised version eventually later submitted on 26 September 2013 for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD; Since completed with data from 31 European States and presented in person to the T-PD Plenary Session on 15 th October 2013. Officially restricted and due to be formally published on-line by the Council of Europe after final corrections and proof-reading before end December 2013, this Report was leaked to Statewatch by unknown persons in September

2013 following its being made available to T-PD members. That 26 September 2013 version is available at http://www.statewatch.org/news/ and specifically downloadable at http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf

[11] Why we need to reform the EU data protection rules? Data Protection reform. Frequently Asked Questions, MEMO/12/41 Brussels, 25 January 2012, http://europa.eu/rapid/press-release_MEMO-12-41_en.htm.

[12] The 1874 Privacy Act (5 U.S.C.A. § 522a) requires the Federal Government to use fair practice in the collection and use of information about USA citizens and it is designed to prevent federal agencies from disclosing certain personal information contained in their records. In application of this text, federal agencies may not release government records without first obtaining consent from the persons who are referred to in those records. Every individual maintains the right to inspect federal agency records, correct mistakes and add important details. In the event that individual's right is infringed under this law, he or she can sue the federal government for monetary damages or a court order directing the agency to obey the law.

[13] REIDENBERG, J.R. (2000). "Resolving Conflicting International Privacy Rules in Cyberspace", 52 *Stradford Law Review*.

[14] The Group submitted its final Report in May 2008 (Council Note 9831/08, Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection, final.

[15] USA Patriot Act, 2001, Pub. L. 107-54, 115 Stat. 272.

[16] Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission, 30 May 2006.

[17] Rooted in the United States Department of Health, Education and Welfare's seminal 1973 Report, "Records, Computers and the Rights of Citizens" (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S.A. States, as well as in those of many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies. See, also guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008- 01.pdf.

[18] 20 U.S.C. § 1232g; 34 CFR, part 99.

[19] Data brokers are companies whose business is collecting and selling information about individuals, companies, markets, etc. Their clients include both private-sector businesses and government agencies.

[20] Schrems v. Data Protection Commissioner (Case C-362/14).

Bibliography

BIRNHACK, M.D. (2008). "The EU Data Protection Directive: An engine of a global regime", n° 24, Computer Law & Security Report.

COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION (2013). "A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes", Office of Oversight and Investigations Majority Staff, Staff Report for Chairman Rockefeller, December 18, available at: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

DWORK, C., MULLIGAN, D.K. (2013). "It's not privacy if it's not fair", in *66 Stan. L. Rev. Online* 35, September.

EPIC, Electronic Privacy Information Centre- White House (2013). Consumer Privacy Bill of Rights.

GUNASEKARA, G. (2009). "The 'final' privacy frontier? Regulating Trans-border data flows", n° 17 (2), *International Journal of Law and Information Technology.*

DE HERT, P. & GUTWIRTH, S. (2009). "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in GUTWIRTH, S. Et AL (eds.) *Reinventing Data Protection?* Springer Science.

DE HERT, P. & PAPAKONSTANTINOU, V. (2013). "Three scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, preferably a UN Agency?", in *I/S, A Journal of Law and Policy for the Information Society,* vol 9:2.

THE SECRETARY´S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, Department of Health, Education and Welfare (1973). The HEW Report on American Records, Computers and the Rights of Citizens.

KAMARINOU, D. (2013). "International transfers of personal data and corporate compliance under Directive 95/46/EC, the Draft Regulation and the international community: Part 1", Comms. L. 2013, 18(2).

KUNER, CH. (2009) "Developing an Adequate Legal Framework for International Data Transfers", in GUTWIRTH, S. Et AL (eds.) *Reinventing Data Protection?* Springer Science.

MARCINKOWSKI, B. (2013). "Privacy paradox(es): in search of a transatlantic data protection standard", *74, Ohio State Law Journal,* 1167.

McBRIDE N., SOTTO L.J. & TREACY, B. (2013). "Privacy and data security: the future of the US-EU Safe Harbour", *Practical Law*, Thomson Reuters.

MOBILE ECOSYSTEM FORUM, MEF (2015). "Global consumer trust Report. Understanding the impact of privacy & security on mobile apps and services".

PEW RESEARCH CENTRE (2015). "Americans' views about data collection and security", survey, May, available at:
http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

REGAN, P.M. (1999). "American business and the European Data Protection Directive: Lobbying strategies and tactics", in BENNETT, C.J. & GRANT, R. (eds.): *Visions of Privacy: Policy Choices for the Digital Age*".

ROTENBERG, M. (2001). "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)", in *Stanford Technology Law Review.*

SOLOVE, D.J. & SCHWARTZ, P.M. (2009). *Privacy, Information and Technology.* New York. Aspen Publishers.

WRIGHT, D., DE HERT & P., GUTWIRTH, S. (2011). "Are the OECD Guidelines at 30 showing their age?", in 54 (2), *Communications of the ACM*.