LUISS SCHOOL OF GOVERNMENT

Working Paper Series

THE SHORTCOMINGS OF THE EU FRAMEWORK FOR TRANSNATIONAL DATA TRANSFERS AND THE NEED FOR AN INTERNATIONALIST APPROACH

SOG-WP43/2017 ISSN: 2282-4189

Martinho Lucas Pires

Printed in Italy, November 2017

LUISS School of Government

Via di Villa Emiliani, 14

00197 Rome ITALY

email: sog@luiss.it

web: www.sog.luiss.it

ABSTRACT

The continuous technological evolution of the digital economy, for which there are no physical barriers and borders, has led to an increase of cross-country data flows and transfers. This creates a normative issue when transfers are transnational, i.e. when they occur between different legal orders. This difference in regulatory status, combined with the easiness that data is transferred to different countries risks undermining the level of protection of personal data at a global level. This paper attempts to show that there are normative shortcomings of the current EU framework for transnational data transfers, particularly regarding its practical effectiveness and balance of three social interests — individual privacy rights, economic freedom and national security — at stake. This paper also argues that, due to the importance of data transfers in today's world, it is necessary to refuse a nationalistic approach and instead adopt an internationalist output for better protection of privacy rights globally.

Keywords*: Transnational data transfers, Schrems case, Balancing of rights, Data protection legal framework, Global law*

The author would like to thank Prof. Dra. Catarina Botelho and the participants of the Católica Graduate Leal Research Conference for their comments and discussion of this paper. This article was produced with the support of a scholarship from Fundação para a Ciência e Tecnologia (FCT).

This working paper constitutes the development of that presented during the 2017 Summer school on "Parliamentary democracy in Europe", organised in the framework of the Jean Monnet Module on "Parliamentary accountability and technical expertise: budgetary powers, information and communication technologies and elections" (PATEU).

AUTHOR INFORMATION

Martinho Lucas Pires is a lawyer and PHD candidate at Nova Law School Lisbon in EU Law and invited assistant lecturer of Public Law at Católica Law School Lisbon. He holds a Bachelor and LLM Degree from Católica Law School Lisbon. He was a Grotius Research Scholar at University Michigan Law School in the US. He writes and works in the fields of constitutional theory, European Union Law, Economic and Monetary Union, and Data Protection and Internet law.

Contact Information:
martinholucaspires@fd.unl.pt
martinholucaspires@fd.lisboa.ucp.pt

TABLE OF CONTENTS

I. INTRODUCTION: DIGITAL AGE AND DATA TRANSFERS

We are currently living in an era of wide digitalization of human practices. By this we mean that, instead of the use of physical instruments, these practices now use (and / or are based on the use of) digital technologies, such as smartphone applications, computer programs, website registries, etc. Users, economic agents and public servants insert their data into these programs and software. Information, composed of codes, algorithms and binary languages, is then stored in servers and processed. This technological shift has led to a revolutionary change in the way we communicate and, therefore, of how we interact with one another, from mere social to more commercial interactions.

Therefore, there is a great degree of (necessary) data transfers in this stage of the digital era. As a report from the United Nations Conference on Trade and Development states, «[e]very day, vast amounts of information are transmitted, stored and collected across the globe, enabled by massive improvements in computing and communication power».[1] A major characteristic of this new global setting is the velocity and apparent lack of boundaries for data transmission. With a simple mouse click or screen touch we can send a message to another person located in a different country, maybe even on the other end of the globe.

This development and consequent increase of transnational data transfers poses serious challenges from a legal perspective. Although the World Wide Web does not know no barriers, the same is not true regarding regulation of social interactions and economic activity. States are not only separated by physical borders; they are also separated by strong legal differences.

Law is idiosyncratic, part of the wider cultural *acquis* of a given political community[2]. It sets out the object and method of regulation in accordance with the specific interests and concerns of that specific community. This means that regulation of transnational data transfers shall be structured in accordance with different interests. For some political communities, the interest of regulating data transfers shall strongly take into account the economic potential of technology development, i.e. setting out legislation with minimum regulation criteria in order to enable the greater number of transfers. For other political communities, national security issues shall be the key point, i.e. setting out legislation that enables the State to access, albeit within certain limits, personal data in order to protect the integrity of the community as whole. Finally, other communities, while taking into account the importance of the first two principles, consider that the core of regulating transnational data transfers shall be to protect the data itself, i.e. the rights of individuals to the privacy of their personal data.

As such, we face a difficult legal conundrum. Transnational data transfers are a necessary reality in the globalized world we live in. We can say that it is already inherent to the way communication happens in the world today. However, it is very difficult to limit these transfers by physical means. At the same time, there is a difference in effect concerning the rights and other sets of legal protections afforded to users from one legal order to another. In this sense, it is possible that there can be wide discrepancies in legal protection that may jeopardize individual rights of users, such as their right to privacy. There are also high thresholds of protection of individual rights that shall impact the development of economic activity and, also, affect national

[1] United Nations Conference on Trade and Development (2016), p. xi
[2] COTTERELL, Roger (2006), p. 97-105

security issues. Intelligence activity requires the possibility to investigate and collect data, albeit within limits concerning individual rights.

Therefore, regulation of transnational data transfers has a strong impact in the way that not only rights are protected, but also economic and security relations are established between different countries. The different balance set out in different legal orders regarding this "triangle" impairs the effective resolution of this global problem. Neither one of these three interests is properly protected in a wider perspective, but instead is dependent on national regulation, the level of protection of which that can vary greatly. The concern is that while regulatory models are based in a national, protectionist perspective it will always be difficult to achieve an effectively balanced model for regulating this issue that affects citizens in the whole world. In this sense, an internationalist, global legal approach to the problem could provide a better, more effective and balanced regulatory model.

The present paper has the purpose of critically analyzing the current approach to transnational data transfers regulation by looking at the EU legal framework on this topic. The EU has a very sophisticated legal framework of data protection and transnational data transfers, a model that has been replicated in other States, such as Japan or Israel[3]. However, we believe that the model is indicative of the difficulties of having an over-national approach to a global issue. The model as it stands has important shortcomings concerning the balance achieved between the efficient allocation of the interests at stake. These shortcomings may prove critical in setting a predictable structure that, in the long term, can protect individual rights effectively and guarantee strong intelligence cooperation and stable economic relations between countries.

The paper is structured as follows. In the first section, we shall describe the EU normative model of transnational data transfers and its framework. The model is set out in Directive 95/46/CE ("the Directive") — to be replaced in 2018 by Regulation 2016/679, also known as the GDPR — and in the interpretative criteria set out by the CJEU in the *Schrems* case. In the second section, we shall present and discuss the importance of the triangle of interests subjacent to transnational data transfers: development of economic relations and global prosperity, protection of national security and intelligence activities and guaranteeing of individual rights, mainly the right to privacy. In the third section we shall look at the EU model from a critical perspective, taking into account the balance of interests set out in the previous section and the impact of the *Schrems* judgment. In the fourth section, we shall consider the problems set out from what we consider a nationalistic, protectionist approach to regulating transnational data transfers. We shall conclude by making the case for an internationalist approach to the regulation of global data transfers.

II. The EU legal framework for transnational data transfers: law and case law

The EU legal framework for transnational data transfers is set out in Chapter IV, articles 25 and 26 of the Directive. According to article 25, paragraph one, data transfers to a third country

[3] United Nations Conference on Trade and Development (2016), p. 13 and p. 32-34.

can occur only if the receptive country provides an adequate level of data protection. Apart from this situation there can only be transfers following the conditions set in the derogations established in article 26[4]. Therefore, the Directive sets that transnational data transfers from the EU to third countries outside these situations are prohibited.

Evaluation of the adequate level of data protection of the third country shall be done by the European Commission. As paragraph 2 of article 25 states, this evaluation «shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations». The Commission shall take into account several criteria when performing this evaluation, such as: the nature of the data; the reason for treatment and its duration; the place of departure of data and to where it shall be sent after treatment; the legal framework of data protection in the receiving country, both in national law and in international commitments; and «the professional rules and security measures» that are in place in the receiving country's territory. Following this evaluation, the Commission shall adopt a decision (an adequacy decision) stating if the third country provides or not an adequate level of data protection, in accordance with article 25 number 6. Therefore, by adopting the decision the Commission is permitting general data transfers to that specific third country.

The Directive has been recently amended by the GDPR, which shall enter into force on May 18 of 2018, according to its article 99. Regulation of transnational data transfers is set out in articles 44 to 50 of Chapter V of the GDPR. The general rule remains that transnational data transfers are prohibited unless there is either an adequacy decision by the Commission or an exception like ones that were set out in article 26 of the Directive. However, article 45 of the GDPR sets out a reinforced list of criteria for the Commission to consider when evaluating the adequacy level of data protection in a third country. It adds to the criteria set out in article 25 of the Directive:

«the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred»

and

«existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for

[4] Article 26 sets out a series of situations where transnational transfers are allowed even if the receptive country does not provide an adequate level of data protection. These cases — points a) to f) — take into account situations where the transfer has the purpose of safeguarding an important interest of the data subject, such as in judicial procedures or in cases of medical information. Also, according to article 26 number 2, transnational transfers shall not be blocked if made within the framework of private agreements that set out effective data protection rules in contractual clauses.

assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States (…)»

The Commission shall also take into account the existence of binding international agreements regarding data protection issues. The GDPR also establishes a set of derogations for transnational transfers outside the scope of an adequacy decision in articles 46 and 49. The exceptions still take into account the individual interest at stake in the transfer as the justification for it to occur even if the third country does not guarantee an adequate level protection. The GDPR adds to the former framework the more open, and general criteria that if there are sufficient safeguards concerning rights and adjudication of rights for that particular transfer, then the transfer can go through.

The main interpretative issue in the EU's legal framework for transnational data transfers concerns the meaning of the concept of what is an adequate level of protection. It was up for to the Commission, following the criteria set out in the Directive, to make a decision regarding this notion. However, since the criteria were rather open, the Commission enjoyed a certain amount of discretion when evaluating the adequacy of a third country's system of data protection.

The question regarding the meaning of the concept of an adequate level of protection was discussed before the CJEU in the *Schrems* case[5]. This case concerned a judicial controversy in Irish courts between an Austrian citizen, Maximilian Schrems, and Ireland's Data Protection Commissioner. The claimant considered that it was necessary to reevaluate if the USA was or not providing an adequate level of data protection, after the Snowden revelations exposed the practice of mass surveillance and collection of data by the American intelligence services. In this sense, the Irish Data Protection Commissioner, according to Schrems, had to analyze his request and see if this was the case, something that the Commissioner refused to, partly because there was a previous adequacy decision enacted by the EU regarding the USA[6]. Maximilian Schrems decided to appeal against the Commissioner's decision to the Irish High Court.

This Court considered that the Snowden revelations offered damaging evidence of the US's practice against individual rights of privacy as protected by Irish and European law[7]. The Irish Court then referred this question to this CJEU: could the Data Protection Commissioner refuse to analyze a claim on the basis of an existent adequacy decision by the European Commission?

The CJEU started by answering this question in a positive manner, stating that to understand otherwise would mean that individuals would be less protected in face of violations to their rights of privacy by third countries. It would also unfairly restrict the role of national authorities of data protection[8]. The EU Court then moved to look into the Commission's adequacy decision regarding the USA in order to assess its validity *vis-à-vis* the Directive and general principles of EU law. In order to do so, the CJEU had to define what is should be understood as being an adequate level of protection.

---

[5] CJEU case C-362/14, *Maximilian Schrems* (2015)

[6] Commission Decision 2000/520 (2000). The adequacy decision considered that the principles of Safe Harbor presented by the USA — principles relating to protection and treatment of personal data that US companies would have to comply with — were sufficient to guarantee an adequate level of protection.

[7] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraphs 30 to 35

[8] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 66

The EU Court stated that a third country has an adequate level of protection if it has in place a legal framework of protection of fundamental rights that is «essentially equivalent» to the EU's framework[9]. This does not mean that the third country's framework has to be identical to the European one. What is required is that the third country needs has effective legal tools in place to protect the rights of users in a way that is substantially similar to the protection granted to individuals by EU law[10]. The Commission's discretion in this field are, therefore, restricted to this criteria of equivalence, and should be supervised accordingly[11].

The CJEU develops this idea further by stating three characteristics that a legal framework of data protection equivalent to the EU's should have. The first characteristic concerns the *efficiency* of the framework itself. In this sense, there shall exist in the third country sufficient legal tools and instruments in place that can, in practice, detect, deter and punish any infringement to its own norms[12]. One important element here for the EU Court is that the rules in place must apply not only to private parties, such as companies, but also to public authorities, such as government agencies. The second characteristic concerns the *exceptional* character of any infringement. Interferences with the right of privacy and the right of data protection — articles 7 and 8 of the Charter respectively — can only occur if they are legal, necessary and proportional. This means that interferences shall pursue a goal of general interest, be defined by clear and precise rules, set minimum guarantees of data protection and finally, applied only if strictly necessary and according to a proportionality assessment[13]. The third and final characteristic concerns the *judicial means of redress* available to individuals. According to the CJEU, it is necessary that there are effective options available to individuals to react against interferences in their rights of privacy and data protection. The Court states that «legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter[14]».

Through the application of these criteria, the CJEU found that the adequacy decision regarding the US was invalid in face of EU law[15]. The Court argued that the Commission did not justify that the US legal framework of data protection guaranteed an essentially equivalent level of data protection[16]. The CJEU stated that according to the adequacy decision it seems that in the US the principle of national security has primacy over legal principles of data protection[17]. The adequacy decision also implied that this supremacy is excessive and imbalanced because it does not present rules destined to limit the effect of interference of US authorities when assessing

---

[9] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 73
[10] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 74
[11] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 78
[12] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 81
[13] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 91. The rationale of the CJEU in this case regarding the application of a strict proportionality assessment to infringement of the right to privacy had been previously applied in the *Digital Rights* case. See CJEU joined cases C-293/12 and C-594/12, *Digital Rights* (2014). For an analysis of the case, see GRANGER, Marie-Pierre, and IRION, Kristina, (2014), pp. 835-850.
[14] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 95
[15] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraphs 105 and 106
[16] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 98
[17] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraphs 84 and 85

personal data for national security purposes[18]. The fact that US legislation allowed for indiscriminate mass collection of data shows that interference with the individual right to privacy is not made under strict necessity and proportionality. Finally, the CJEU pointed to the lack of judicial means of redress available to individuals *vis-à-vis* data collection by US intelligence agencies as not being compatible with the right to an effective judicial remedy stated in article 47 of the Charter[19].

III. The EU legal framework and the immediate consequences of Schrems: Privacy Shield

The EU legal framework for transnational transfer of data after *Schrems* can be summoned as follows[20]. Transnational data transfers are, in principle, forbidden, unless they fall into one of the derogations set in the Directive – and in the future, in the GDPR. The derogations allow for transfers in specific individual situations. Transnational transfers of data to a third country can also be allowed if there is an adequacy decision enacted by the Commission. An adequacy decision represents an assessment by the Commission of a third country's legal framework of data protection. If the Commission finds that this framework is adequate — i.e. that the third country offers an essentially equivalent framework of protection of fundamental rights regarding treatment and collection of personal data — the decision allows for general transfers of data between the EU and the third country. Finally, when assessing the adequacy of the third country's framework, the Commission must assert that the fundamental rights set out in the Charter — in particular articles 7 (right to privacy), 8 (right to data protection) and article 47 (right to an effective judicial remedy) — are duly protected, in accordance with the CJEU's jurisprudence on the matter.

The *Schrems* case ended with the CJEU declaring that the adequacy decision regarding transnational transfers to the USA was invalid in face of EU law, for failing to comply with the adequacy criteria and with the duty of the Commission to justify, in substance, its evaluation[21]. The Court stroke down the legal act and did not introduce any interim measures. In this sense, after *Schrems* there was no permission, in face of EU law, to transfer data from the EU to the USA[22].

In August 2016 this situation was corrected when the Commission issued a new adequacy decision[23]. The USA reformed the *Safe Harbor* principles, setting out new obligations for companies and developing some of the former principles. The current framework is named *Privacy Shield* and follows the same structure of the *Safe Harbor,* albeit more developed[24]. Within this new setting of principles, there were also statements by American authorities explaining the

---

[18] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 88
[19] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 95
[20] For another overview, see OJANAN, Tuomas (2017), pp. 15-18.
[21] The CJEU did not considered the Safe Harbor principles *per se* as invalid; it opted to consider the adequacy decision and the action of the Commission in this regard. It was an indirect way of assessing the US system of protection.
[22] See MAY, Lisa and MABERRY, J. Scott (2015).
[23] For a history of the negotiations, see VOSS, Gregory W. (2011), p. 11. For an understanding of the American model of regulating data protection, see HASTY, Robert *et alii* (2013).
[24] Commission Decision 2016/1250 (2016).

rules regarding the powers and limits of action of US intelligence agencies regarding individual data collection.

It is possible to read from the adequacy decision that the Commission has made a visible effort to justify its assessment that the US has an adequate level of protection. This effort is seen not only in the dimension of the adequacy decision — 112 pages long, with 155 explanatory clauses; the *Safe Harbor* adequacy decision was 47 pages long, with 11 explanatory clauses — but in the content. In several points of the decision the Commission refers directly to the *Schrems* decision and the interpretative criteria of the CJEU. The enactment of the adequacy decision regarding the USA was welcome due to the important economic interests at stake. After *Schrems* there was uncertainty regarding the future of transnational data transfers and what type of framework was going to be put in place. The USA is one of the most important economic actors at the forefront of digital businesses and technology; not to have an adequacy decision could jeopardize the development of business ties with US companies.

However, the *Privacy Shield* adequacy decision has been criticized by experts[25], academics[26] and politicians[27] alike. These critics state, in general, that the Privacy Shield does not answer properly to the criteria set out by the CJEU in *Schrems* and, therefore, does not offer sufficient guarantees of protection of fundamental rights of EU citizens. Although it presents new principles and rules for companies to comply with, the American framework remains based on auto-certification and doubts regarding the extent of powers of US intelligence authorities remain[28]. Furthermore, it does not present sufficient guarantees for individuals to react against interference by American intelligence agencies[29]. In a nutshell, critics argue that the US does not present a regulatory framework of protection of privacy and data rights of European individuals that is essentially equivalent to the protection those individuals benefit from EU law.

There have been already attempts at challenging the Privacy Shield adequacy decision in the CJEU[30]. This is not the place to enter into a discussion of the Privacy Shield *per se* and see the merits of these critiques. Suffice to say that, in our opinion, there are two spheres of relations to consider.

One is the private sphere — i.e. relations between companies / entrepreneurs and consumers — and the other the public sphere — i.e. relations between US public authorities and individuals. The adequacy decision presents in general a structured, reasoned and developed set of justifications and arguments supporting adequacy of the US system. This is particularly true in comparison with the *Safe Harbor* adequacy decision. From the point of view of the private sphere, there are more precise duties for companies to comply with, and more assurances of regular supervision provided by American authorities (the Federal Trade Commission and the Department of Commerce). There is also an extensive list of judicial mechanisms available to individuals to upheld their rights against possible interferences by private companies. From the point of view of the public sphere there is also an improvement in explaining the limits and checks to the powers of intelligence agencies, as well as the guarantees of individuals to challenge them. However, the

[25] Article 29 Data Protection Working Party (2016) and EDPA (2016)
[26] WISMAN, Tijmen H.A. (2017), pp. 365-366; and MONTELEONE, Shara and PUCCIO, Laura (2017), pp. 31-36
[27] European Parliament (2017)
[28] Article 29 Data Protection Working Party (2016), p. 57; EDPA (2016) p. 7
[29] Article 29 Data Protection Working Party (2016), p. 57; EDPA (2016), p. 11
[30] Politico (2016); EurActiv (2016)

principle of national security can still override *Privacy Shield* principles in the US[31]. There are situations in which the limits of this supremacy are not clear, particularly regarding collection of data[32]. Finally, there are also doubts regarding effective judicial protection of EU citizens against interferences by US authorities, particularly regarding the independence of the *Privacy Shield* Ombudsperson, set out under the administrative structure of the Secretary of State.

Therefore, there are shortcomings, as WISMAN and MONTELEONE and PUCCIO state, that raise some doubts regarding the viability of the adequacy decision for the long term.

IV. The policy-normative interests regarding transnational data transfers

There are three general policy and normative interests that regulation of transnational data transfers should take into account[33]. These interests are: the development of economic relations and global prosperity, protection of national security and protection of individual rights, in particular the right to privacy.

Development of economic and commercial activity through technological evolution can be seen from multiple perspectives. There has been the emergence and incorporation of digital companies that have as their core business the provision of web, app based digital services. Examples of this are companies such as Google or Amazon that provide e-mail accounts, cloud businesses, online shopping or other communicative tools. But even more traditional industrial companies and economic sectors of activity have had to adopt to digitalization in one or many ways. This usually includes the setting of digital communication channels with their clients, either through e-mail, app or an internet profile account. One strong example nowadays is the emergence of companies operating on financial technology areas, also known as Fintech, regarding particularly the provision of financial and banking services[34].

The common characteristic of how digitalization has affected economic actors is the increase in the use, request, collection and treatment of personal data of individual clients at a massive scale. In order to provide their services — either industrial or digital in nature — clients must send certain elements regarding their person, such as age, address or marital status, and in some cases their images, and also specific elements relating to the particular business relation. In this sense, commercial companies — as well as public bodies — have become keepers of large amounts of personal data. It is also important to notice that technological development has enabled the provision of economic services between economic agents and consumers that are geographically apart. Technology, in this sense, permits (and fosters) the globalization of businesses.

The importance of digital economy and the digitalization of economy as a whole cannot be overestimated. According to reports, their effect in investment and growing is already very

[31] Commission Decision 2016/1250 (2016), p. 59
[32] See for example Commission Decision 2016/1250 (2016), pp. 14-15 and p. 19
[33] Discussion of these three interests is very explicit in the wider discourse surrounding data protection. See, for example, United Nations Conference on Trade and Development (2016) pp. xi-xiv; and KUNER, Christopher (2011), particularly pp. 6-9.
[34] See for a consideration of all these manifestations, the recommendations of the Strategic Policy Forum on Digital Entrepreneurship (2016)

expressive and with tendency to grow[35]. The future of economic activity shall occur in the digital realm or at least with recourse to a significant digital interface. With the incorporation of multinational companies, and the easiness of accessing or providing services anywhere in the world to another part, transnational data transfers become a key element for fostering global economic development.

The second policy interest concerns national security issues. The prosecution of internal justice and national security by police bodies, the military and intelligence agencies represents another important social interest to take into account when regulating transnational data transfers. Access to communication data issued by computers or smartphones can allow law enforcement authorities to analyze not only to the content of those communications, but also to find the location and follow the movements of the communicators. Therefore, access to digital servers and databases is a useful and effective tool for achieving the goals of policing and prevention of crimes and threats to national security[36].

Two realities demonstrate the importance of access to private data by national intelligence agencies. The first is the use of internet-based communication services by organized criminal and / or terrorist networks. These organizations can have several cells around the world. Communication, recruitment and training of their members can be achieved through social media and the use digital equipment. Because these entities target attacks in several States, a combined police effort between different national bodies requires that data can be transferred and shared among them, regarding the monitoring and location of suspects. This effort, due to the nature of counter-intelligence and policing activity, has often to be done in secrecy, at the expanse of transparency[37].

The second reality concerns the emergency of digital crimes or cyber-crimes. These acts concern committing a crime through digital means — such as credit card fraud, or theft, or invasion of privacy, to name but a few. In this year of 2017, there have been several of these events, when groups of hackers from unknown origins attacked the servers of several companies around the world, requesting ransoms in exchange for not deleting information contained in the servers[38]. The rise of cybercrime requires the use of digital technologies and access to private information in order to locate and find criminals. It also requires thatsharing, transfer of data between different national polices, and agencies in order to better tackle these threats.

The third policy (and normative) interest to take into account concerns the protection of personal liberties. Technological developments, increase of the digitalization of the economy and the collection and monitoring of personal data for security purposes affect individuals. The easiness and intuitiveness of digital communication, along with continuous requisition of personal information has put personal data at risk and, therefore, the individual's right to privacy[39]. This is so because the user, as the consumer, holds a vulnerable position *vis-à-vis* the commercial undertakings that request his or her data for commercial purposes. At the same time, the

---

[35] According to the United Nations, digital businesses related to data shall have global markets worth of up to 126 billions. See United Nations Conference on Trade and Development (2016) p. xi.

[36] See, for example, the OSCE Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments (2012).

[37] On secrecy and national security, see SCHULHOFER, Stephen (2013).

[38] WIRED (2017).

[39] The right to privacy is one of the most important hallmarks of liberalism. See RICHARDS, David A. (1988); RUBENFELD, Jeb (1989); DeCEW, Judith (2015; and COLE, David and FABBRINI, Federico (2016), pp. 6-8.

individual's data is subject to possible unwanted collection and treatment by police and intelligence authorities[40]. Both these situations can occur internally, i.e. national authorities of and /or companies incorporated in the same legal order of the individual; and externally, i.e. national authorities of a foreign state and / or companies incorporated in a foreign legal order.

It is in this last point data that individual rights in principle will be more vulnerable. Individuals can use the commercial services of a company located in another legal system. By having their data transferred to a foreign country, they shall be subject to the laws of the State in which the company holding data is located. These laws may offer a different level of protection than the one afforded to the individual in his or her own national legal order. Not only that, but in case there is an illicit interference with an individual right the claimant will most likely have to physically travel to that State and set out legal actions there, facing procedures done in a different language, having to deal with a different legal order. There is a problem of protecting the *other*, the foreigner, in terms of data regulation[41].

V. The complicated balance between policy and normative interests

Regulation of transnational data transfers has, therefore, these three main interests to protect. On one hand, transnational data transfers are a necessary part of economic development and of current commercial practices. On the other hand, the emergence of sophisticated criminal and terrorist networks with global reach requires the use of data collection mechanisms and cooperation between different intelligence agencies. Finally, collection of data either by private companies or national States have important implications for the protection and safeguard of individual rights of privacy. In this sense, to regulate transnational data transfers requires a difficult balance these three interests. It is necessary to regulate: for example, from an economic perspective, to provide stability and market effectiveness for companies and other economic agents; from a national security to provide clear and precise powers to intelligence agencies to act and be held liable; and, most important, to protect individual rights. The way in which this regulation can achieve a satisfactory balance is far from obvious.

To put it in more technical terms of constitutional theory, we have in this situation a potential conflict between two individual rights — the right to develop an economic activity and the right to privacy — and a public interest — protection of national security. Adjudication of fundamental rights consists in a balancing act between conflicting and competing interests[42]. This competition generally occurs between the prosecution of a collective interest — e.g. protection of the security of national citizens vis-à-vis external threats — and a fundamental right that is affected by that same prosecution — e.g. the right to privacy. Departing from a liberal theory of rights, it is important in this scenario to understand the status of each conflicting interest / right in face the other. Regulation of transnational data transfers shall be set through balance between these competing and often conflicting interests.

---

[40] FABBRINI, Federico (2015-II), p. 8-10.
[41] As noted by COLE, David and FABBRINI, Federico (2015), p. 16.
[42] KUMM, Matias (2007), p. 133-141.

There are in these point two challenges, of conceptual and practical nature. The first challenge concerns the nature of the collective and individual interests at stake. On one hand, we have a fundamental right, from the core of the liberal tradition of rights: privacy. This right, briefly, concerns the freedom of the individual to have a private sphere, an autonomous space of his personality that is intimate and, therefore, he can shed from being made public. In other words, it is one of the strongest rights of individual protection that is in a liberal society[43]. On the other hand, we have the protection of the community's well-being in face of danger and harm. The prosecution of national security — the duty to maintain order and "peace" — is one of the important tasks of the State[44]. Finally, we have an economic interest. It is difficult to understand what this economic interest is, from a normative conceptual point of view[45]. Is it a right? Economic rights include the freedom to contract and to pursue an economic activity. Nevertheless, the role of these rights is weaker than with the first-generation rights. Is it, then, a collective interest? The interest of allowing a free market that shall, in principle, foster competition and demand and produce wealth that, in turn creates the possibility to generate resources for a given political community. However, it is too abstract as an interest and from a liberal standpoint, a difficult goal to achieve.

In sum, we are dealing with a conceptual and practical challenge of a conflict between a "strong" individual right, a "strong" collective interest, and a difficult categorization of what can be seen as an individual right or a collective interest. This conceptual difficulty weakens, in practice, the claim this economic right or interest might have. However, the conceptual and practical challenge remains. Although rights are trumps or shields, they are subject to infringement if such infringement is not only legal but also legally justified[46]. The challenge is in finding the proper justification (and in, the case of the difficulty of economic rights, the proper legitimacy of the interest), usually through a proportionality assessment.

This brings us to the second challenge. Adjudication of collective interests *vis-à-vis* individual rights is usually done in a judicial form. This means that the final definition of the balance is in the hand of courts, faced with a specific situation in which this conflict arises. The balance can be set *a priori* — for example, with legislation that explains or takes into account the effects on the sphere of fundamental rights — but it can be challenged afterwards in a judicial claim. The exercise of defining the balance is made within a concrete situation. This is so because fundamental rights are optimizations of values[47], or principles[48], as open-ended axiological claims defined in abstract. Therefore, any regulation that sets out a balance between the interests shall have to pass by the courts — in this case, the CJEU — and subject to its institutional rationale, that follows a different methodological and interpretative approach than the political and administrative one of the bodies enactors of legislation[49].

---

[43] It should be pointed out that the new challenges relating to "privacy" in a digital age. See the United Nations High Commissioner for Human Rights Report (2014).
[44] DUNLAP JR., Charles J., (2012), p. 1057.
[45] On the conceptual discussion (and problem) of economic rights, see WALDRON, Jeremy (2010), and DE VRIES *et alli* (2015).
[46] KUMM, Matias (2007), p. 132.
[47] KUMM, Matias, (2004), pp. 579-582.
[48] DWORKIN, Ronald, (1997), pp. 24-27.
[49] Following the economic theory of institutional choice of KOMESAR, Neil (2011), pp. 1-4.

VI. The balance of interests in the EU legal framework of transnational data protection

We have previously seen how the EU legal framework of transnational data transfers is set out. In the following section, we shall see how these three interests — economic development, national security and fundamental rights protection — are represented in the EU legal framework.

Fostering of the digital economy is one of the goals of a data protection framework, according to the European Commission. The Commission states that «[d]ata has become an essential resource for economic growth, job creation and societal progress. (…) This global trend holds enormous potential in various fields, ranging from health, environment, food security, climate and resource efficiency to energy, intelligent transport systems and smart cities»[50]. The European Parliament also acknowledges that «transfers of personal data between commercial organizations of the EU and the US are an important element for the transatlantic relationships»[51]. The importance of the digital economy is part of the wider strategy for the EU.

National security, on the other hand, is an interest that is not much discussed by the legislative and executive institutions concerning transnational data transfers. The institution that looks more closely into the discussion of national security as a political and legal interest is the CJEU. In *Schrems*, as we previously saw, the Court takes issue with the importance attached to the interest of national security *against* protection of privacy rights in America. The Court states that:

«As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights (…) must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data»[52].

For the CJEU, the balance of interests of EU law is the following. Fundamental rights should be upheld against national security. Only if this former interest is pursued by political actors within requirements of legality, necessity and proportionality, and always guaranteeing a minimum level of protection of privacy rights can it interfere, to a certain extent, with the latter's sphere. In this case, however, the requirements of necessity and proportionality were not satisfied.

Protection of privacy rights of European citizens is the interest that is most referred by the political and executive institutions. As the Commission states, «Respecting privacy is a condition for stable, secure and competitive global commercial flows. Privacy is not a commodity to be traded. (…) In the digital era, promoting high standards of data protection and facilitating international trade must thus necessarily go hand in hand»[53]. The European Parliament also argues that «[transatlantic data] transfers should be carried out in full respect of the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is

[50] European Commission (2017), "Building a European Data Economy" p. 2.
[51] European Parliament (2017), p. 3.
[52] CJEU case C-362/14, *Maximilian Schrems* (2015), paragraph 91.
[53] European Commission (2017), p. 6.

the protection of fundamental rights, as enshrined in the EU Charter»[54]. In addition, as stated in the previous paragraph, protection of privacy rights is the interest that the EU's main judicial institution puts at the forefront, from a legal standpoint.

Therefore, the balance of interests set out in EU law, as established clearly by the CJEU, is the protection of individual rights of privacy[55]. National security is a legitimate public interest that can interfere with the sphere of the rights of privacy, as long as if its pursuance follows criteria of necessity and proportionality, and does not affect a minimum core of the right. Finally, economic development is a political interest, as a goal to be achieved, but that is not taken into account as a legal interest for a balancing perspective. Consequently, the EU shall only accept to transfer data to a third country where this balance is also achieved and set in law.

VII. The shortcomings of the legal framework: a consequence of the model

The position of the CJEU follows a liberal conception of fundamental rights adjudication. In this sense, the right of privacy and the right to data protection prevail over other interests, unless the adjudication of these interests follows the legal criteria of proportionality. This position of the Court has been widely supported by European academics and certain advisory bodies and agencies. It has also been criticized by American academics. The point of critique concerns the balance of interests at stake, and the methodology of the decision[56]. Other actors, such as American politicians and certain economic agents have also expressed their concern over the CJEU's approach, calling it "over-zealous".

We are not interested in discussing the merits of the Court's judgment. Suffice to say that in our opinion the CJEU is taking a coherent approach regarding protection of privacy with its previous decision in *Digital Rights Ireland*. Our main concern, however, has to do with the regulatory *model* of the EU *per se*. In our opinion, the CJEU decision is nothing more than a consequence of the way in which the model is set up.

The EU legal framework for allowing transnational transfer of data is based on a model of recognition. This means that the EU shall only allow general transfers of data to third countries if it recognizes that the third country has a legal framework of data protection that is adequate — i.e. «essentially equivalent» to its own legal framework of protection. In this sense, the EU is basically upholding its legal framework *vis-à-vis* other countries. The underlying message is: if you want our data, then have rules that, in essence, protect privacy rights as much as ours do. It is a case of regulatory recognition — recognition of a legal framework that is similar to the EU's. And in that sense, the EU model upholds a certain balance of interests, in which fundamental rights cannot be

[54] European Parliament (2017), pp. 3-4.
[55] OJANEN, Thomas (2017), p. 29.
[56] The most poignant critique has been made by EPSTEIN, Richard (2016-I). See the rejoinder by SCHEININ, Martin (2016) and the response by EPSTEIN, Richard (2016-II). See also EDGAR, Timothy H., (2015) and BRILL, Julie, and MAXWELL, Winston, (2016).

trumped by national security objectives unless prosecution of those interests is proportional, in accordance with the criteria set by the CJEU[57].

The problem lies in this point. The EU model sets out an obligation for the Commission to consider only legal frameworks of third countries that offer not only the same *degree* of protection but also (and particularly) the same *balance* of interests that the EU sets. And this is something far more complicated to assess and to guarantee, because of the contextual considerations that fundamental rights adjudication and balance of interests entail, as we previously saw. One thing is to have this as a limit for prohibiting transfers to States that are less or not liberal at all political systems, with dubious application of rule of law principles and fundamental rights adjudication. But another, completely different, is to assess other liberal democracies, such as the USA, where there are fundamental rights and freedoms, but also competing interests that are politically and socially legitimate[58]. The balance of adjudication between these rights and interests may differ from the one set in the EU due to social and cultural traditions and idiosyncrasies. Adjudication may vary also not only in content but also in method. At the same time, the general principles of law and reasoning are fairly similar, since they stem from a liberal and democratic background.

We can call this the third challenge of fundamental rights adjudication. First, the difficulty of, *in abstract*, define the balance. Second, the fact that final adjudication of the balance rests in the hands of a judicial body. Third, the fact that the balance of interests can be substantially different due to context — not only of the case that is being discussed, but also (and more crucially) the legal context in which the dispute in front of the Court arises.

The risk is that this discrepancy may be difficult to solve through this model. Balances of principles and fundamental interests are culturally contextual. The model of recognition and evaluation of equivalence is subject to changes in this balance. In this sense, if the balance shifts, equivalence shall no longer exist — as the CJEU stated in *Schrems*, when assessing the adequacy decision and the balance set there and in the US intelligence practice of the time. This creates a problem due to the instability that the model is subject to. This instability affects not only economic and diplomatic relationships, because of the efforts to negotiate new data transfer agreements (as the *Privacy Shield* saga proved) but, particularly, individuals. Without agreement of data transfers it is the data of individual EU citizens that shall be subject to less protection and rights, particularly with regards to their relation with American companies. Another problem is the possibility to create tensions of legal and political diplomacy. Relations between the EU and other countries — in the particular case, with the US — could be affected by this situation.

In sum, the EU's legal framework for transnational data transfers is highly protective of fundamental rights, and rightly so. However, it is based on a system of equivalence that is prone to be unstable in the long term, thus creating a regulatory loophole that affects all interests worth defending at stake.

---

[57] The problem is also the seemingly "uncompromising approach" of the CJEU to data privacy, as pointed by FABBRINI, Federico (2015), p. 20 and OJANEN, Thomas (2017), p. 25-29.

[58] On the USA's constitutional balances or adjudications see NOLTE, Georg (2003) and the several contributions to this monograph; on proportionality in the US and in the EU see also KUMM, Matias (2007), pp. 150-152; on the right to privacy, more specifically, see WHITMAN, James Q. (2003), p. 89-91, and COLE, David, and FABBRINI, Federico (2015), p. 10-15.

VIII. Conclusion: the case for an internationalist approach

Global problems require global solutions. Transnational data transfers is a reality in today's world. The problems associated with it affect not only European citizens abroad, but also other countries' citizens. A reality requires regulation and a strong legal framework to protect the interests of individuals and States.

The recent decision of the CJEU on privacy rights related with data transfers and treatment and the enactment of an updated legal framework demonstrate the importance that data transfers have for European judicial and political actors alike. The model puts at its center the unequivocal protection of the rights of privacy and data protection of individuals, *vis-à-vis* interests such as national security.

Despite its qualities, the model has also important shortcomings. It is a model based on a protectionist idea of normative and regulatory recognition. Transnational data transfers can only occur in general when the receiving country has an essentially equivalent level of protection of individual rights to the EU — that may count as setting out the same balance of interests of the EU legal order. This may prove difficult to achieve in a long-term basis, even in other liberal and democratic countries. Evidence of this is the Safe Harbor /Privacy Shield saga involving the USA. If the balance of interests is not the same, then equivalence shall not exist. Due to the important economic and political role of the USA regarding technologic and digital industries of communication, the lack of a stable channel of data transfer may put at peril the rights of privacy of European citizens in the long term.

This is why there should be a shift in the regulatory approach, from a nationalistic to an internationalist (or globalist) stance. This means the urgency to set up an international normative model for regulating data transfers and privacy security between different countries and different legal systems. It would be in the best interest of all parties involved, for the sake of stability and guarantee of the interests to be protected. In fact, a globalist approach could help set out a framework dealing with the three complex interests at stake — economic relations, national security and rights of privacy — and setting a level playing field between all countries with clear and transparent rules, rights, and obligations. It could also guarantee a mechanism of adjudication of individual rights with more effective protection for citizens of participant countries[59].

The problem with this approach is that it requires all interested countries to agree on its terms. It shall likely require compromises from all parties — and internal procedures of approval that, in the case of the EU, will have the participation of judicial entities. Nevertheless, it is a risk worth taking. It would be long-term solution for setting up a strong, efficient framework for data transfers, enabling economic growth, answering to national security issues and with the possibility of setting a high standard of protection of privacy and data protection rights. And it would also strength legal relations between legal orders that could prove useful for other matters, such as human rights law or trade[60].

---

[59] We follow therefore the position of COLE, David and FABBRINI, Federico (2015), p. 15-18.

[60] An example that can be seen in the influence of regulatory practices of the EU on the US and vice-versa. See FAHEY, Elaine, (2014), pp. 368-384.

BIBLIOGRAPHY

BRILL, Julie, and MAXWELL, Winston, (2016), "Criticisms of Privacy Shield Fail to Recognize Shortcomings of Europe's Own Intelligence Laws", *Bloomberg BNA,* in https://www.bna.com/criticisms-privacy-shield-n57982074106/ (last access October 11, 2017)

COLE, David and FABBRINI, Federico, (2015), "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders", *iCourts Working Paper Series*, number 33, pp. 1-19

COTTERRELL, Roger (2006), *Law, Culture and Society: Legal Ideas in the Mirror of Social Theory*, Ashgate, Hampshire

DeCEW, Judith, (2015), "Privacy", T*he Stanford Encyclopedia of Philosophy,* Edward N. Zalta (ed.), in https://plato.stanford.edu/archives/spr2015/entries/privacy/ (last access October 11, 2017)

De VRIES *et alli* (2015), "Research Paper on the Categorization of Economic Rights", *BEU Citizen,* in http://beucitizen.eu/wp-content/uploads/Deliverable_5_1_final.pdf (last access October 11, 2017)

DUNLAP JR., Charles J., (2012), "Ethical Issues of the Practice of National Security Law: Some Observations", *Ohio Northern University Law Review*, volume 38, pp. 1057-1095

DWORKIN, Ronald, 1997, *Taking Rights Seriously,* Harvard University Press, Cambridge

EDGAR, Timothy H., (2015), "Schrems vs. Data Protection Commissioner: Some Inconvenient Truths the European Court of Justice Ignores", *Lawfare Blog,* in https://www.lawfareblog.com/schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores (last access October 11, 2017)

EPSTEIN, Richard (2016-I), "The ECJ's Fatal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices", *European Constitutional Law Review*, volume 12, number 2, pp. 330-340

EPSTEIN, Richard (2016-II), "The Deepening EU Blindness on Privacy: A Pointed Response to Professor Martin Scheinin", *European Constitutional Law Review*, volume 12, number 2, pp. 349-352

FABBRINI, Federico (2015), "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court", *iCourts Working Paper Series*, number 19, pp. 1-23

FABBRINI, Federico (2015-II), "Introduction: Privacy and National Security in the Digital Age", *Tilburg Law Review*, Volume 20, number 1, pp. 5-13

FAHEY, Elaine, (2014), "On the use of law in transatlantic relations: Legal dialogues between the EU and US", *European Law Journal*, volume 20, number 3, pp. 368-384

GRANGER, Marie-Pierre, and IRION, Kristina, (2014), "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection", *European Law Review*, volume 39, number 6, pp. 835-850

HASTY, Robert *et alli*, 2013, "Data Protection Law in the U.S.A.", *Advocates for International Development,* in http://www.a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf (last access October 11, 2017)

KOMESAR, Neil K., (2011), "The Essence of Economics: Behavior, Choice and Comparison - Essay One 'The Basic Thesis with Lessons from the Economic Analysis of the Common Law'", *University of Wisconsin Legal Studies Research Paper,* number 1173, pp. 1-29

KUMM, Matias, (2004), "Constitutional Rights as Principles: On the Structure and Domain of Constitutional Justice", *I.CON,* volume 2, number 3, pp. 574-596

KUMM, Matias, (2007), "Political Liberalism and the Structures of Rights: On the Place and Limits of the Proportionality Requirement", *Law, Rights and Discourse: Themes from the Legal Philosophy of Robert Alexy,* George Pavlakos (ed.), Hart Publishing, Oxford, pp. 131 - 166

KUNER, Christopher, (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", *OECD Digital Economy Paper*, number 187, pp. 1-39
MAY, Lisa and MABERRY, J. Scott (2015), "The Schrems Decision: How the End of Safe Harbor Affects Your FCPA Compliance Plan", *Global Trade Law Blog*, in http://www.globaltradelawblog.com/2015/11/12/the-schrems-decision-how-the-end-of-safe-harbor-affects-your-fcpa-compliance-plan/ (last access October 11, 2017)
MONTELEONE, Shara and PUCCIO, Laura (2017), "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules", *European Parliament Research Service*, pp. 1-36
NOLTE, Georg (ed.), (2003), "European and U.S. Constitutionalism", *Seminar of the European Commission for Democracy Through Law*, in http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-STD(2003)037-e (last access October 11, 2017)
OJANEN, Thomas, (2017), "Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union", *Surveillance, Privacy and Transatlantic Relations*, COLE, David *et alli* (ed.), Hart Publishing, Oxford, pp. 13-30
RICHARDS, David A., (1988), "Liberalism, Public Morality and Constitutional Law: Prolegomenon to a Theory of the Constitutional Right to Privacy", *Law and Contemporary Problems,* volume 51, number 1, pp. 123-150.
RUBENFELD, Jeb, (1989), "The Right of Privacy", *Harvard Law Review*, volume 102, number 4, pp. 737-807
SCHEININ, Martin (2016), "Towards Evidence-based Discussion on Surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review*, volume 12, number 2, pp. 341-348
SCHULHOFER, Stephen (2013), "Oversight of national security secrecy in the United States", *New York University Public Law and Legal Theory Research Paper Series Working Paper*, number 21.
VOSS, Gregory W., 2016, "The Future of Transatlantic Data Flows: Privacy Shield or Bust", *Journal of Internet Law*, vol. 19, number 11, pp. 8-18.
WALDRON, Jeremy, (2010), "Socioeconomic Rights and Theories of Justice", *NYU School of Law Public Law Research Paper,* number 10-79, in https://ssrn.com/abstract=1699898 (last access October 11, 2017)
WHITMAN, James Q. (2003), "Human Dignity: The Social Foundations", *Seminar of the European Commission for Democracy Through Law*, in http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-STD(2003)037-e (last access October 11, 2017)
WISMAN, Tijmen H.A., (2017), "Privacy, Data Protection and E-Commerce", *EU Regulation of E-Commerce: A Commentary*, LODDER, Arno R. *et alli*, Edward Elgar Publishing, Gloschester, pp. 349-382.

Institutional documentation and reports:

Article 29 Data Protection Working Party, (2016) "Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (last accessed October 11, 2017)
CJEU case C-362/14, *Maximilian Schrems* (2015)
CJEU joined cases C-293/12 and C-594/12, *Digital Rights* (2014).
EDPA, (2016) "Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision" de 30 de Maio de 2016", in https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf (last accessed October 11, 2017)

European Commission (2017), "Communication on Building a European Data Economy", in https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy (last access October 11, 2017)
European Parliament, (2017), "Motion for a Resolution on the Adequacy of the Protection Afforded by the EU-US Privacy Shield", B8-0235/2017, in http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2017-0235+0+DOC+PDF+V0//EN (last access October 11, 2017)
OSCE (2012) *Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments,* in http://www.osce.org/eea/96398?download=true (last access October 11, 2017)
United Nations Conference on Trade and Development (2016), *Data protection regulations and international data flows: Implications for trade and development*, United Nations Publication, Switzerland, in http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last access October 11, 2017)
United Nations High Commissioner for Human Rights, (2014) *The Right to Privacy in the Digital Age,* Report, in http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last access October 11, 2017)
Strategic Policy Forum on Digital Entrepreneurship (2016) "Accelerating the digital transformation of European industry and enterprises", *European Commission,* in http://ec.europa.eu/DocsRoom/documents/15856/attachments/1/translations/en/renditions/native (last access October 11, 2017)

News articles:

Politico, (2016), "Privacy shield data agreement challenged before EU court", in http://www.politico.eu/article/privacy-shield-data-agreement-challenged-before-ecj/ (last access October 11, 2017)
EurActiv, (2016), "EU-US Privacy Shield pact faces second legal challenge", in http://www.euractiv.com/section/digital/news/eu-us-privacy-shield-pact-faces-second-legal-challenge/ (last access October 11, 2017)
WIRED, (2017), "The Biggest Cybersecurity Disasters of 2017 So Far", in https://www.wired.com/story/2017-biggest-hacks-so-far/ (last access October 11, 2017)

SCHOOL OF GOVERNMENT
LUISS Guido Carli

The LUISS School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions.

The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organizational leadership).

For more information about the LUISS School of Government and its academic and research activities visit. www.sog.luiss.it

SUBMISSION GUIDELINES

LUISS School of Government welcomes unsolicited working papers in English and Italian from interested scholars and practitioners. Papers are submitted to anonymous peer review. Manuscripts can be submitted by sending them at sog@luiss.it . Authors should prepare complete text and a separate second document with information identifying the author. Papers should be between 8,000 and 12,000 words (excluding notes and references). All working papers are expected to begin with an indented and italicised abstract of 150 words or less, which should summarise the main arguments and conclusions of the article. Manuscripts should be single spaced, 11 point font, and in Times New Roman.

Details of the author's institutional affiliation, full postal and email addresses and other contact information must be included on a separate cover sheet. Any acknowledgements should be included on the cover sheet as should a note of the exact length of the article. A short biography of up to 75 words should also be submitted.

All diagrams, charts and graphs should be referred to as figures and consecutively numbered. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text. Tables should be placed at the end of the file and prepared using tabs. Any diagrams or maps should be supplied separately in uncompressed .TIF or .JPEG formats in individual files. These should be prepared in black and white. Tints should be avoided, use open patterns instead. If maps and diagrams cannot be prepared electronically, they should be presented on good quality white paper. If mathematics are included, 1/2 is preferred.

It is the author's responsibility to obtain permission for any copyrighted material included in the article. Confirmation of Workinthis should be included on a separate sheet included with the file.

SOG WORKING PAPER SERIES

The LUISS School of Government aims to produce cutting-edge work in a wide range of fields and disciplines through publications, seminars, workshops, conferences that enhance intellectual discourse and debate. Research is carried out using comparative approaches to explore different areas, many of them with a specifically European perspective. The aim of this research activities is to find solutions to complex, real-world problems using an interdisciplinary approach. LUISS School of Government encourages its academic and student community to reach their full potential in research and professional development, enhancing career development with clear performance standards and high-quality. Through this strong focus on high research quality, LUISS School of Government aims to understanding and influencing the external research and policy agenda.

This working paper series is one of the main avenues for the communication of these research findings and opens with these contributions.

WP #1 – Sergio FABBRINI, *Intergovermentalism and Its Outcomes: the Implications of the Euro Crisis on the European Union* SOG-Working Paper 1, January 2013.

WP #2 - Barbara GUASTAFERRO, *Reframing Subsidiarity Inquiry from an "EU value-added" to an "EU non encroachment" test? Some Insights from National Parliaments' Reasoned Opinions*. SOG-Working Paper 2, February 2013.

WP #3 - Karolina BOROŃSKA-HRYNIEWIECKA, *Regions and subsidiarity after Lisbon: overcoming the 'regional blindness'?*, SOG-Working Paper 3, March 2013.

WP #4 - Cristina FASONE, *Competing concepts in the early warning mechanism*, SOG-Working Paper 4, March 2013.

WP #5 - Katarzyna GRANAT, *Institutional Design of the Member States for the Ex Post Subsidiarity Scrutiny*, SOG-Working Paper 5, March 2013.

WP #6 – Cecilia Emma SOTTILOTTA, *Political Risk: Concepts, Definitions, Challenges*, SOG-Working Paper 6, April 2013.

WP #7 – Gabriele MAESTRI, *Il voto libero: la necessità di regole chiare e trasparenti sul procedimento preparatorio e di un contenzioso che decida rapidamente,* SOG-Working Paper 7, July 2013.

WP #8 – Arlo POLETTI & Dirl DE BIÈVRE, *Rule enforcement and cooperation in the WTO: legal vulnerability, issue characteristics, and negotiation strategies in the DOHA round*,, SOG-

Working Paper 8, September 2013.

WP #9 - Sergio FABBRINI, *The Parliamentary election of the Commission President: costraints on the Parlamentarization of the European Union*, SOG-Working Paper 9, October 2013.

WP #10 - Lorenzo DONATELLI, *La disciplina delle procedure negoziali informali nel "triangolo decisionale" unionale: dagli accordi interistituzionali alla riforma dell'articolo 70 del regolamento del Parlamento Europeo,* SOG Working Paper 10, October 2013.

WP #11 - Mattia GUIDI & Yannis KARAGIANNIS, *The Eurozone crisis, decentralized bargaining and the theory of EU institutions*, SOG Working Paper 11, November 2013.

WP #12 - Carlo CERUTTI, *Political Representation in the European Parliament: a Reform Proposal*, SOG Working Papers 12, January 2014.

WP #13 – Dessislava CHERNEVA-MOLLOVA, *The EP's rules of procedure and ther implications for the Eu institutional balance*, SOG Working Papers 13, February 2014.

WP #14 - Luca BARTOLUCCI, *The European Parliament and the 'opinions' of national parliaments*, SOG Working Papers 14, February 2014.

WP #15 - Leonardo MORLINO, *Transitions to Democracy. What We Know and What We Should Know*, SOG Working Papers 15, April 2014.

WP #16 - Romano FERRARI ZUMBINI, *Overcoming overlappings (in altre parole...oltre 'questa' Europa)*, SOG Working Papers 16, April 2014.

WP #17 - Leonardo MORLINO, *How to assess democracy in Latin America?*, SOG Working Papers 17, April 2014.

WP #18 - Nicola LUPO & Giovanni PICCIRILLI, *Some effects of European Courts on national sources of law: the evolutions of legality in the Italian legal order*, SOG Working Papers 18, May 2014.

WP #19 – Cristina FASONE, *National Parliaments under "external" fiscal constraints. The case of Italy, Portugal, and Spain facing the Eurozone crisis*, SOG Working Papers 19, June 2014.

WP #20 - Elena GRIGLIO & Nicola LUPO, *Towards an asymmetric European Union, without an asymmetric European Parliament*, SOG Working Papers 20, June 2014.

WP #21 - Ian COOPER, *Parliamentary oversight of the EU after the crisis: on the creation of the "Article 13" interparliamentary conference*, SOG Working Papers 21, August 2014.

WP #22 – Anne PINTZ, *National Parliaments overcoming collective action problems inherent in the early warning mechanism: the cases of Monti II and EPPO*, SOG Working Papers 22, October 2014.

WP #23 – Valentina Rita SCOTTI, *Religious freedom in Turkey: foreign models and national identity*, SOG Working Papers 23, January 2015.

WP #24 – Davide A. CAPUANO, *Overcoming overlappings in the European Union (entia non sunt multiplicanda praeter necessitatem …)*, SOG Working Papers 24, February 2015.

WP #25 – Francesco ALICINO, *The road to equality. Same-sex relationships within the european context: the case of Italy*, SOG Working Papers, July 2015.

WP #26 – Maria ROMANIELLO, *Assessing upper chambers' role in the EU decision-making process*, SOG Working Papers 26, August 2015.

WP #27 – Ugljesa ZVEKIC, Giorgio SIRTORI, Alessandro SABBINI and Alessandro DOWLING, *United Nations against corruption in post-conflict societies*, SOG Working Papers 27, September 2015

WP #28 – Matteo BONELLI, *Safeguarding values in the European Union: the European Parliament, article 7 and Hungary*, SOG Working Papers 28, October 2015

WP #29 - Ludovica BENEDIZIONE & Valentina Rita SCOTTI, *Equally victims? Post-revolutionary Tunisia and transitional justice*, SOG Working Papers 29, November 2015.

WP #30 - Marie-Cécile CADILHAC, *The TTIP negotiation process: a turning point in the understanding of the European parliament's role in the procedure for concluding EU external agreements?*, SOG Working Papers 30, December 2015.

WP #31 - Francesca BIONDI & Irene PELLIZZONE, *Open or secret? Parliamentary rules of procedures in secret ballots*, SOG Working Papers 31, December 2015.

WP #32 - Giulio STOLFI, *Tempi (post-)moderni: nuovi impulsi normativi europei alla prova delle sovrapposizioni*, SOG Working Papers 32, January 2016.

WP #33 – Diane FROMAGE, *Regional Parliaments and the early warning system: an assessment*

six years after the entry into force of the Lisbon treaty, SOG Working Papers 33, April 2016.
WP #34 – Luca DI DONATO, *"A behavioral principal-agent theory to study corruption and tax evasion,* SOG Working Papers 34, July 2016.

WP #35 – Giuseppe PROVENZANO, "*The external policies of the EU towards the southern neighbourhood: time for restarting or sliding into irrelevance?*", SPG Workin Papers 35, September 2016.

WP #36 – Rosetta COLLURA, *"Bruegel, EU think tank in the EU multi-level governance",* SOG Working Papers 36, October 2016.

WP #37 - Franco BRUNI, Sergio FABBRINI and Marcello MESSORI, *"Europe 2017: Make it or Break it?"*, January 2017.

WP #38 - Alina SCRIPCA, "*The Principle of Subsidiarity in the Netherlands and Romania. Comparative Assessment of the Opinions Issued Under the Early Warning Mehanism*", SOG Working Papers 38, April, 2017.

WP #39 - Eleonora BARDAZZI, Omar CARAMASCHI, "*Italian and European Citizens' Initiatives: Challenge and Opportunities*", SOG Working Papers 39, April 2017.

WP #40 - Diane FROMAGE and Renato IBRIDO, "*Democratic Accountability and Parliamentary Oversight the ECB. The Banking Union Experience*", SOG Working Papers 40, June 2017.

WP #41 – Marco CECILI, *"La sussidiarietà e l'early warning system tra diritto e politica. Il caso della c.d. "Direttiva Tabacco" del 2014"*, SOG Working Papers 41, September 2017.

SCHOOL OF GOVERNMENT
LUISS Guido Carli