The International Data Transfer Framework and its Political Consequences: a Practical Approach

DIOGO BRITO FONSECA[*]
INÊS PEREIRA AIRES[*]
ISABEL CHOWDHURY[*]
MARGARIDA PERES PEREIRA[*]

Abstract: The international data transfer framework presents itself with many shortcomings. This paper is aimed at analysing European law and determining the practical approach of the courts. It begins by mapping out the troubles of information circulation and legal basis for the regime. There are three paradigmatic cases analysed, *Schrems I* and *II* and *El Gizouli v SSHD*, regarding the European data transfers to the United States and its expected future repercussions in the law. A final recent case, regarding the Lisbon Municipality and Russian Embassy to Portugal, is used to analyse the practice of data protection by state authorities.

Keywords: *Data transfer; General Data Protection Regulation (GDPR); Police directive; Schrems.*

---

[*] Licenciado em Direito e Pós-graduado em Direito da Proteção de Dados pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Advogada-estagiária. Licenciada em Direito e Pós-graduada em Direito da Proteção de Dados pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito -Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Consultora jurídica. Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

[*] Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Frequenta o Mestrado em Direito - Especialização em Direito Empresarial e Tecnologia na NOVA School do Law.

Resumo: O regime da transferência de dados internacional apresenta várias lacunas. Este texto visa descortinar o Direito Europeu e a demarcação da abordagem prática dos tribunais. Mapeia as dificuldades da circulação de informação e a base legal do regime. Revê-se três casos paradigmáticos: *Schrems I* e *II*, e *El Gizouli v SSHD*, como exemplos de transferência de dados europeus para os E.U.A., e as repercussões esperadas na lei. Analisa-se ainda o caso da transferência de dados entre o Município de Lisboa e a embaixada da Rússia em Portugal para averiguar o rigor da proteção de dados pelas autoridades governamentais.

Palavras-Chave: *Transferência de dados; Regulamento Geral sobre a Proteção de Dados (RGPD); Diretiva de Polícia; Schrems.*

1. Introduction

The digital economy[1] has pushed data flows into an unprecedented and large scale level, generating a whole industry around it, the data industry, aided by the way the internet has globalised trade. Practically every website we visit on a daily basis asks for data in exchange for their content, through cookies,[2] making them effective intermediaries in the data trade, and allowing them to continue to live by selling that data to interested parties or using it for their own benefit. The truth is: our current digital footprint contains almost every digitalizable aspect of our lives. It is extremely difficult, if not almost

1 "The digital economy is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people, organizations, and machines that results from the Internet, mobile technology and the internet of things (IoT)", in *What is digital economy?*, Deloitte. Available at: <https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html>

2 "Cookies are small files that websites send to your device that the sites then use to monitor you and remember certain information about you — like what's in your shopping cart on an e-commerce site, or your login information. These pop-up cookie notices all over the internet are well-meaning and supposed to promote transparency about your online privacy." in STEWART, Emily, *Why every website wants you to accept its cookies*, Vox, 2019. Available at: <https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy>

impossible for a person to live a normal life without leaving a digital footprint. And this is where concerns rise: around the possible malicious and legally dubious purposes data about these individual, private citizens may be used.

The GDPR states as the reasoning behind its conception the protection of natural persons, under article 8(1) of the Charter of Fundamental Rights of the European Union

(EUCFR) and article 16(1) of the TFEU, and the particular conditions of increased cross-border data flows due to the creation of the EU internal market. With its creation in 2016, it is now the leading data protection framework in the world and has inspired many other countries to adopt similar ones.[3]

Given the context we previously mentioned, it is natural that data management is needed, especially when data is being exchanged between two legal orders that offer the data subject different levels of protection. The legal regime for data transfers is defined in articles 44 and following. This part of the GDPR assumes particular relevance due to the importance and goal the EU has set as to protecting natural persons as much as possible within its jurisdiction. This is reflected in the adequacy decision criteria denounced in article 45, allowing data transfers to proceed only when the third country in the negotiation is deemed to have a data protection framework that "ensures an adequate level of protection".[4]

In this context, and throughout this paper, we wish to explore the complexities and vicissitudes of this framework. We will focus on the practical application it has, how it influenced politics, was used as a tool for political manoeuvring and abuse and reflect the lack of international understanding in a search for a mutual response to data transfer problems.

---

3 Greenleaf, Graham, *Global data privacy laws 2019: 132 national laws & many bills*, 157 Privacy Laws & Business International Report, 14-18, 2019. Available at: <*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593*>

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 45(1)

2. Democracies facing the Information Wars

We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war.
William Perry, 19th US Secretary of Defense

If until nowadays the Government's main concern was external threats, today is cyberspace security and defense. The Portuguese Institute of National Defense defines cyberwar as a "conflict between two or more nations or between different groups within a nation where cyberspace is the battlefield".[5] When related to data, we can talk about "information warfare", meaning any action to deny, exploit, corrupt or destroy the enemy's information and its functions"".[6] The information manipulation problem is universal. Government information management is related to national security and international reputation and, in democracies, where the circulation of information is free, this issue is particularly dangerous. Information is not just an instrument, but a vulnerability source.

2.1 Information warfare

"Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale".[7] The internet, as an open global resource and international cooperation, has a huge role in society, "enhances and expands the possibilities of data acquisition, information defence, and information disruption, and makes it easy to reach both the citizens of a given country and the international".[8] "Fake news", "disinformation", "propaganda", are all terms used to describe this phenomenon.

---

5 (Free translation)

6 Borden, Col Andrew, *What is Information Warfare?*, USAF, p. 1. Available at: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>

7 Nato, *Media – (Dis)Information – Security*. Available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf>

8 Ibid.

Historically, and according to the US Army Heritage and Education Center[9]information warfare has been achieved with psychological operations and electronic operations. For the purpose of controlling the American propaganda machine, Franklin Roosevelt established the Office of War Information. As an example, around 1943/1945 the Army Air Forces use to make strategic radio transmissions coordinated with the bombing.

The use of information as a weapon, in the context of a political war, has some risks. "Today, the collection, analysis, and sale of personal information powers global economies; information is, as the dictum goes, power, but we can also argue that it acts as a modern-day currency".[10]

We are currently living in an information era, where "technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities".[11] According to the Recital (16) of the GDPR, the Regulation "does not apply to […] activities concerning national security". However, in the current digital economy, the main economic actors are corporations, especially technology companies.

As GDPR mentions, in Chapter V, data protection rules do apply in international data transfers and the supervisory authorities "shall take appropriate steps to […] the protection of personal data and other fundamental rights and freedoms".[12]

2.2 Data transfers

There have been some attempts to prevent data transfer malicious threats, for example, in 2006 the EU launched a Directive that "required the providers of publicly available electronic communications services and networks to retain traffic and location data belonging to individuals or legal entities for up to two years".[13] [14]

9 U.S. Army Heritage and Education Center, *A Return to Information Warfare*

10 Strategy Bridge, *Thucydides in the Data Warfare Era*, 2018. Available at: <https://thestrategybridge.org/the-bridge/2018/5/30/thucydides-in-the-data-warfare-era>

11 GDPR Recital (6)

12 GDPR Article 50

13 Bruegel, *Data transfers under the threat of terrorist attacks*, 2018. Available at: <https://www.b ruegel.org/2015/12/data-transfers-under-the-threat-of-terrorist-attacks/>

14 In April 2014, however, the ECJ concluded that the Directive interferes with the

The recent attacks, together with the Schrems[15] decision, challenge the ability to transfer data. Faced with the manipulation of information, the consequences are now taken seriously, States have taken several measures ranging from organisational design to the regulation of the media, through the role of parliaments and public awareness.[16] The definition of "information manipulation" is not consensual and the difficulty of qualifications leaves room for arbitrariness in determining the illegal nature of some actions. Although there is no common sense on what qualifies as an act of "cyberterrorism", according to the US Federal Bureau of Investigation (FBI), cyberterrorism is the "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against noncombatant targets by subnational groups or clandestine agents". Cyberterrorism is a powerful tool because "Internet […] provides a global pool of potential recruits and donors. Online terrorist fundraising has become so commonplace that some organizations are able to accept donations via the popular online payment service PayPal."[17]

Regarding data protection, the EU adopted, in 2005, the European Union Counter-Terrorism Strategy that comes down to four principal ways of approach: i. prevention; ii. protection; iii. investigation; iv. post-attack responses. The current EU Counter-Terrorism Strategy belongs to the EU Global Strategy that identifies cyber threats as one of the main threats that the EU is facing.[18] The EU cooperates with international organisations and bodies to develop strategies for these threats. International data transfers are essential to daily business operations.[19] Even though there are many ways to secure the transmission of data, one of the main concerns is related to data collection and

---

fundamental rights of EU citizens and violates the right to protection of personal data.

15 P. 9.

16 Marangé, Céline, QUESSARD, Maud , *Les guerres de l'information à l'ère numérique*, PUF

17 Kaplan, Eben, *Terrorists and the Internet*, Council on Foreign Relations, 2009. Available at: <https:// www.cfr.org/backgrounder/terrorists-and-internet>

18 European Security & Defence, *EU Counter-Terrorism Strategy*, 2020. Available at: <https://euro-sd.com/ 2020/02/articles/16153/eu-counter-terrorism-strategy/>

19 Deloitte, *GDPR Update: The future of international data transfers*. Available at: <https://www2.deloit te.com/ch/en/pages/risk/articles/gdpr-the-future-of-international-data-transfer.html>

use. Data collection is vulnerable to several risks. The device's connectivity leaves data more vulnerable to a breach, and when a data breach takes place, the entire system is at risk of being compromised.[20] Nowadays, over 130 jurisdictions[21] have some form of privacy and data protection legislation and almost one in three companies fall under the EU GDPR jurisdiction.[22] But different jurisdictions have different points of view. "The EU stands firmly for the interests of the individual. […] Europeans must provide positive consent for the ways their data is used, and they have the right to access and erase that data, as well as the "right to be forgotten." In the opposite corner sits the United States and the giant US corporations that trade in personal data for profit, and whose practices have expanded largely unchecked. One ideology puts the control of personal data in the hands of the individual, the other cedes control to the corporation. (A third approach is state control of data, which is emerging as China's social credit system, though that remains as yet an internal policy.) But these differing views about data protection cannot jostle for dominance for much longer. As trade grows increasingly global, it's becoming clear that personal data crosses borders far too easily for contrasting models to co-exist".[23] Understanding the importance of the data and protecting it as an asset in order to manage possible threats has a more positive impact than trying to avoid cyber risk.

States security against cyber attacks must be a priority to the governments. Data as a weapon and data as a goal is a reality. The use of information to manipulate ideas or cyber-attacks whose intention is to steal private and confidential information are a risk to societies. When democracies are the target, these threats have even more impact. Every day huge amounts of data are collected and processed, and the use of this information is great for society, for example, when used in scientific and/or social research. But, as with everything, it also has a "dark side", such as fake news and massive control.

---

20 Hanover, *How Data Collection Impacts Cybersecurity*, 2020. Available at: <https://www.hanrec.com /post/how-data-collection-impacts-cybersecurity>

21 i-Sight, *A Practical Guide to Data Privacy Laws by Country*, 2021. Available at: <https://www.i-sig ht.com/resources/a-practical-guide-to-data-privacy-laws-by-country/>

22 Ibid.

23 Pendergats, Tom*, The Next Cold War Is Here, and It's All About Data*, 2018. Available at: <https://w ww.wired.com/story/opinion-new-data-cold-war/>

One of the typical examples is the governments' elections, where news has an important role in opinion-making and, consequently, in the ballots. Most of the digital infrastructure is managed by the private sector and the development of, for example, surveillance tools are *subsequently used to attack fundamental liberal principles like press freedom*.[24]

Concerning AML/CFT[25] and economic effects of information warfare, since money laundering requires market manipulation[26] and criminal intention, that also causes damages to democracies, especially economically. "AML/CFT controls mitigate the adverse effects […] and promotes integrity and stability".[27]

2.3 Recommendations & suggestions

Since the world is becoming more and more connected, is a global strategy against "unprotected" data transfers, including both States and Corporations concerns and contributions. Regulating without strangling technology improvements must be one of the purposes, as well as public investment in human resources. "In its latest annual Cyber Security Breaches Survey the Government Department for Digital, Culture, Media and Sport (DCMS) reported that cyber security is a high priority for 78% of businesses, up from 74% last year."[28] As Marrietje Schaake said, democratic nations must ensure that the digital ecosystem operates according to democratic values.[29]

Another suggestion**,** and agreeing with James Coker, is the development of stronger transparency requirements.[30] "It is easy to see that information

---

24 Coker, James, *#BHEU: How to Create a Safe and Democratic Digital Infrastructure,* Info Security. Available at: <https://www.infosecurity-magazine.com/news/bheu-safe-democratic-digital/>

25 Anti-Money Laundering/Combating the Financing of Terrorism.

26 International Monetary Fund, *Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)*. Available at: <https://www.imf.org/external/np/leg/amlcft/eng/>

27 Ibid.

28 Hallett, Steve, "How Data Collection Impacts Cybersecurity", in Hanover, 2020. Available at: <https://www.hanrec.com/pos t/how-data-collection-impacts-cybersecurity>

29 Coker, James, "BHEU: How to Create a Safe and Democratic Digital Infrastructure", in Info Security Magazine, 2021. Available at: <https://www.infosecurity-magazine.com/news/bheu-safe-democratic-digit al/>

30 Ibid.

warfare is no less complex than traditional warfare".[31] The transversal nature of this subject/discussion is obvious and one of the concerns is "the opacity that rules over the choices made by the largest platforms, to which neither legislators nor users have access".[32] "Information warfare is all about measures to improve (or degrade) the efficiency of decision-making".

"The maximum theoretical efficiency depends on the amount and quality of data available and the amount of ambiguity in the data".[33] From what we have exposed, the collaboration between democracies is crucial, aligned with company resources and knowledge.

3. The Impact of Schrems I and Schrems II in International Data Transfers

3.1 Legal context

The GDPR, safeguards "any transfer of personal data which are undergoing processing or are intended for processing after transfers to a third country or an international organisation"[34]. The transfers of personal data need to rely on one of the legal basis for transfers provided by the GDPR under Chapter V, but as well as all the rules and principles stated in this regulation.

Under the European Union data protection law, three mechanisms allow for personal data to be transferred from a Member State to a third state: (1) transfers can be based on a Commission decision finding that the third state ensures an "adequate level of protection"[35]; (2) in the absence of the prior point, the transfer can take place when it is accompanied by "appropriate safeguards"[36], like Standard Contractual Clauses, SCCs, or Binding Corporate

31 Burns, Megan, "Information Warfare: What and How?", 1999. Available at: <http://www.cs.cmu.edu/~./burnsm/InfoWarfare.html>

32 Marangé, Céline, Quessard, Maud, "Les guerres de l'information à l'ère numérique", PUF, 2021

33 Borden, Andrew, "What is Information Warfare?", USAF, p. 5. Available at: <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>

34 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, article 44. Available at: <Art. 44 GDPR – General principle for transfers - General Data Protection Regulation (GDPR) (gdpr-info.eu)>

35 Article 45 of the General Data Protection Regulation, GDPR

36 Article 46 GDPR.

Rules, BCRs[37]; and lacking this safeguards, based on certain derogations for specific situations[38].

Many of the most interesting cases in privacy from the last few years have dealt with international data transfers, such as the *CompuServe*[39], the *Lindqvist*[40], the *Passenger Name Record*[41] cases, and even the *Microsoft Warrant*[42] case. As different as those cases might be, they all assumed that there is an established system of how transfers of personal data can be done legally[43], but that understanding was challenged by the Court of Justice of the European Union with the *Schrems*[44] case, arising from Edward Snowden's revelations that the National Security Agency had been operating secret surveillance programmes, which brought the beginning of a development where all the mechanisms for international data transfer are scrutinised in much more detail but also more protective of the specific data carried in the process.

---

37 Article 47 GDPR.

38 Article 49 GDPR.

39 *Compuserve* (1998) 8340 Ds 465 Js 173158/95 (AG München); *Compuserve* (1999) 20 Ns 465 Js 173158/95 (LG München). The case dealt with the liability of the German chairman of the access provider CompuServe for illegal content accessible via the intranet. Available at: <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20M%FCnchen&Datum=28.05.1998&Aktenzeichen=8340%20Ds%20465%20Js%20173158/95>

40 Reference to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against Bodil Lindqvist, Case C-101/01 Lindqvist [2003] ECR I-12971. Clarified the meaning of the provisions relating to transfers of personal data to third countries or international organisations. Available at: <https://curia.europa.eu/ju ris/liste.jsf?num=C-101/01>

41 Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union (Passenger Name Record)* [2006] ECR I-04721; Opinion 1/15 *Concerning the request for an opinion by the European Parliament regarding the agreement envisaged between Canada and the European Union on the transfer of passenger name record data*. Available at: <https://curia.europa.eu/juris/liste.jsf?num= C-317/04&language=en>

42 United States District Court, E.D., Pennsylvania, *Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 2017, 232 F. Supp. 3d 708 (E.D. Pa. 2017). Available at: <https://casetext.com/case/in-re-search-warrant-no-16-1061-m-to-google>

43 Bräutigam, Tobias, "The Land of Confusion: International Data Transfers between Schrems and the GDPR", 2016). Tobias Bräutigam and Samuli Miettinen (eds), 'Data Protection, Privacy and European Regulation in the Digital Age' (Helsinki, 2016), Helsinki Legal Studies Research Paper 46, page 4. Available at SSRN: <https://ssrn.com/abstract=2920181>

44 Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Request for a preliminary ruling from the High Court (Ireland), Case C-362/14 Schrems v Data Protection Commissioner (Grand Chamber, 6 October 2015). Available at: <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>

3.2 Brief overview of Schrems I case: from the (un)safe harbour to the Privacy Shield

Transatlantic data flows between the European Union and the United States, or US, were made possible in 2000 through the Safe Harbour[45] scheme. The Safe Harbour was based on a system of voluntary self-certification and self-assessment of US-based companies that they abide with certain data protection principles combined with some intervention by the public authorities.[46] In practical terms, it was required to the US companies to register their compliance with the Safe Harbour principles with the United States Department of Commerce, while the Federal Trade Commission was responsible for enforcing the agreement, having the European Commission to decide on the recognition of the adequacy of the protection provided by these principles.

The European Commission, after thirteen years, with the breach of trust caused by the American "widespread surveillance of private communications of citizens, companies or political leaders"[47] to the transfer of personal data from citizens of the European Union to the United States, brought to a decision, two years later, that entailed this processing of personal data beyond what is strictly necessary and proportional to the imperatives of national security protection and took the opportunity to clarify the adequacy criterion[48], *Schrems I*.

Maximilian Schrems, an Austrian lawyer, lodged a complaint asking the Irish Data Protection Commissioner to prohibit Facebook Ireland from

---

45 European Commission Decision of 26 July 2000 pursuant to Directive 95/46 on the level of protection afforded by the "safe harbour" principles and the most frequent questions (Faqs) issued by the Department of Commerce of the United States of America (Decision 2000/520/EC). Available at: <2000/518/CE: Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça [notificada com o número C(2000) 2304] (Texto relevante para efeitos do EEE.) - Publications Office of the EU (europa.eu)>

46 Tzanou, Maria, "Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights", page 5, 2020, Available at SSRN: <https://ssrn.com/abstract=3710539>

47 European Commission, Communication from the commission to the European parliament and the council, Rebuilding Trust in EU-US Data Flows, Brussels (27 november 2013), page 2. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF>

48 Tzanou, Maria, page 5, 2020.

transferring his personal data to servers located in the United States,[49] arguing that the law and practice in force in that country, in particular the surveillance activities of intelligence services, did not meet the requirement of the level of adequate protection[50]. The Court of Justice of the European Union issued its decision in 2015, concluding that the United States authorities were able to access the personal data transferred from the European Union Member States and process it beyond the strictly necessary and proportionate to the protection of national security.[51]

So, what was decided, directly, was that the US data privacy regime lacks adequate protection towards the European citizens, due to: (1) the regime including different sources like the US Constitution, the Supreme Court case law, federal legislation, State legislation and the theory of torts;[52] (2) the pure nature of self-regulation, without any *ex ante* or *ex post* of a public authority[53]; (3) "adequate level of protection" shall be interpreted as requiring the third country to effectively ensure a level of protection of fundamental rights and freedoms "substantially equivalent" to within the EU,[54] and we cannot argue that a country that has general derogations which makes possible unjustified and unlimited interference with the fundamental rights of data subjects[55], has the necessary level of protection.

The court clarified that a third country has sufficient protection only if it complies with a specific protection scheme for natural persons about the interference with fundamental rights for the purpose of State surveillance,

---

49 EDPS Case Law Digest: Transfers of personal data to third countries, page 8, 2021, . Available at: <https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en>

50 Moniz, Maria da Graça, "A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites", page 258, 2018. Available at: <https://run.unl.pt/bitstream/10362/89180/1/Fonseca_2019.pdf>

51 This discussion can be found in Tzanou, Maria, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' (2017) 17(3) Human Rights Law Review 545. Available at: <https://academic.oup.com/hrlr/article-abstract/17/3/545/3061949>

52 Shaffer, Greggory, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards", 25 Yale Journal of International Law 1, 22, 2000.

53 Moniz, Maria da Graça, 2018.

54 Judgment of the ECJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, (6 October 2015), paragraphs 73 and 74.

55 Judgment of the ECJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, (6 October 2015), paragraphs 87 and 88.

but also showed the lack of legitimacy in inadequate protection against such interference in the several Member States[56] and the lack of guarantee of the protection continuity after the personal data have been transferred to the third country,[57] assuring the fundamental rights and guarantees to which everyone is entitled in the European Union.

It was a "landmark" judgement,[58] but given his, negative financial, impact on the transatlantic trade and the promises made by the US to reform the law and current practises,[59] the European Commission adopted a new decision, known as the Privacy Shield[60] in 2016 to rekindle this connection.

Privacy Shield was adopted to replace Safe Harbour, invalidated in *Schrems I*, in the form of an adequacy decision. It was based on a system of self-certification by which US organisations committed to a set of privacy principles,[61] that included a segment on the access and use of personal data that is transferred under the agreement by the United States public authorities for national security and law enforcement motives. Attached to the draft adequacy decision were seven annexes from US government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations[62], but also strengthening obligations on companies regarding limits on data retention and onward transfers.

---

56 Tzanou, Maria: "The EU's claim as a moral leader in respect for fundamental rights is not always obviousv. "The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security", UJIEL, n.º 31, vol. 80, (2015), p. 87 e ss..

57 G29, "Working document on a common interpretation of paragraph 1 of Article 26 of Directive 95/46 (25 november 2005). Available at: <https://www.pdpjournals.com/docs/88080.pdf.>

58 Kuner, Christopher, "Reality and Illusion in EU Data Transfer Regulation Post Schrems" (March 2016) Cambridge Faculty of Law Legal Studies Research Paper Series, Paper 14/2016. Available at: <https:// papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346>

59 European Commission, "Transatlantic Data Transfer: Restoring Trust through Solid Guarantees", (29 February 2016), page 17. Available at: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3 A52016DC0117>

60 Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. Privacy Shield, Brussels, 12 July 2016, C(2016) 4176 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG>

61 Tzanou, Maria, (2020), page 12.

62 European Commission Unveils EU-U.S. Privacy Shield, EUR. COMM'N (29 February 2016). Available at: <https://ec.europa.eu/newsroom/just/items/30375/en>

A lot of elements in the Privacy Shield showed how hard it was to combine the different notions of privacy between the U.S. and Europe[63], from the lack of central supervisory authority in the US, as expected in the article 51. of the GDPR, to the differences facing structural definitions[64]. Even if the Commission found that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the US, serious concerns were raised as to whether Privacy Shield complies with EU data protection and privacy standards,[65] mainly because the decision was based on US assurances, without any major substantive commitments by the respective authorities to comply with European Union fundamental rights requirements as expressed by the Court of Justice of the European Union in Schrems I.

With all of this in mind, it was expected that new problems would arise by the Commission's failure to resolve the structuring issues for data subjects on this matter, the American data surveillance programmes that were signalled, again, by *Max Schrems* on the *Schrems II* case.

3.3 The Schrems II case: additional protective measures and extraterritorial application

Following the invalidation of Safe Harbour, *Max Schrems*, reformulating his complaint lodged with the Irish Data Protection Authority, asked the Data Protection Commission to suspend his personal data held by Facebook Ireland to Facebook, Inc claiming that these could be made available to US authorities, such as the National Security Agency and the Federal Bureau of Investigation, in the context of surveillance programmes that impede the exercise of the rights

63 Bräutigam, Tobias, (2016), page 159.

64 European Commission, "Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield" C (2016) 4176 final Annexes 1 to 7 (Brussels, 12 July 2016) and Annex II, part II, art. 2 (c)). Regarding the "choice" principles that define the permission level needed to share sensitive data as "affirmative express consent", opt in.

65 See WP29, Opinion 1/2016 of 13 April 2016 on the EU–U.S. Privacy Shield draft adequacy decision WP 238. Available at: <https://www.pdpjournals.com/docs/88536.pdf.>

guaranteed in the Charter of Fundamental Rights of the European Union[66]. The legal framework of the claim this time concerned the data transfers in the U.S. under the Standard Contractual Clauses, SCCs, based on the Decision 2010/87.[67]

On 16 July of 2020, the Court of Justice of the European Union, CJEU, published its *Schrems II*[68] judgement that invalidated the European Commission's Privacy Shield adequacy decision[69]. The court held that the U.S. does not provide a sufficient level of protection, as guaranteed by the GDPR and the EUCFR, having surveillance programmes, such as *PRISM* and *UPSTREAM*, not being limited to the strictly necessary, which results in disproportionate interference with the rights to protection of data and privacy,[70] regarding the lack of actionable rights for European Union subjects against United States authorities and the broader powers conferred upon the U.S. authorities.

Following the Advocate General *Saugmandsgaard Øe's* opinion[71], the court affirmed the validity of the SCC Decision while stipulating stricter requirements for the SCC-based transfers. The Standard Contractual Clauses do not present lawful or unlawful grounds for data transfer, but if the entities seek to transfer data based on this mechanism, they need to ensure that the data subject has a level of protection essentially equivalent to that guaranteed by

66 The articles 7., 8. and 47. of the EUCFR.

67 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39/5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344/100, 'Decision 2010/87').

68 Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Request for a preliminary ruling from the High Court (Ireland). Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=254046>

69 European Parliament, AT A GLANCE, The CJEU judgment in the Schrems II case (2020). Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN .pdf.>

70 Based on article 45(1) of the GDPR and articles 7., 8. and 52.(1) of the EUCFR.

71 Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Request for a preliminary ruling from the High Court (Ireland). Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX: 62018CC0311>

the GDPR and EUCFR, if necessary, with additional, supplementary, measures to compensate any lacunae in the protection of third-country legal systems,[72] provided that the data exporter concluded that the risks, evaluated by risk assessments[73]access to data by the public authorities of the third country could be addressed by these measures.

Christopher Kuner points out that the CJEU "suggests using 'supplementary measures' to protect data under the SCCs but does not explain what measures these could be".[74] The author affirms that, in effect, all the SCCs become "mini adequacy decisions". In my opinion, this complexity can lead companies, especially smaller ones, to avoid this course entirely, while larger ones will be able to afford the expensive legal advice reviewing a foreign nation's surveillance law for compatibility with EU law, smaller firms will not,[75] making this transfer vehicle too complicated for a process that is responsible for a large fraction of data exports from the European Union[76].

As the CJEU did not define what these additional measures were, the European Data Protection Committee, EDPB, approved Recommendation 1/2020[77], following a public consultation, to guide companies on the scenarios where such measures would be available to exporters to ensure the lawfulness of their international transfers. The EDPB provided a non-exhaustive list of

72 European Parliament, AT A GLANCE, The CJEU judgment in the Schrems II case (2020), page 2. Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ ATA(202 0)652073_EN .pdf>

73 Luther., First-aid kit for "Schrems II" compliance (2020). Available at: <https://www.luther-lawfirm.com/f ileadmin/user_upload/OnePager_Erste_Hilfe_Schrems_II_EN.pdf>

74 Kuner, Christopher, The Schrems II judgment of the Court of Justice and the future of data transfer regulation (17 July 2020). Available at: <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>

75 Chander, Anupam, "Is Data Localization a Solution for Schrems II?", Journal of International Economic Law, Forthcoming, page 5, (July 27, 2020). Available at: <https://ssrn.com/abstract=3662626>

76 The International Association of Privacy Professionals surveyed members and reported that "Seven in 10 respondents say their organization transfers data out of the EU to non-EU countries…. The most popular of these tools — year over year — are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-U.S.Privacy Shield arrangement (60%).").

77 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 (18 June 2021). Available at: <https://edpb.europa.eu /system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf>

supplementary measures, which may add to the safeguards found in article 46 GDPR transfer tools, regarding the technical, contractual, and organisational aspect of it that data exporters need to have in mind regarding the context of the transfer[78], the third country law[79] and the transfer tool used[80].

Generally speaking, the Court's analysis in *Schrems II* is unparalleled for the theoretical interrogations about the US surveillance programmes, and is explained by the fact that a detailed description of US national security and surveillance law was included in the Commission's Privacy Shield adequacy decision. Nevertheless, we can argue that the external dimension of extraterritoriality, examination of the foreign law, was an easier task for the Court with respect to the Privacy Shield than with Safe Harbour, as the former explicitly contained the legal bases regarding US authorities' access to personal data.[81] It is argued that the extraterritorial application of data privacy rights must be based on "rules that are reasonably clear and predictable, both about the threshold question of *applicability* and with regard to the *merits*"[82]. In my opinion, *Schrems II* achieves these requirements, because it establishes the applicability of the European Union data protection law to adequacy decisions for international data flows under the GDPR in the light of the EUCFR, but also this case constructed an applicable test to the external interferences, by interpreting Article 52(1) of the EUCFR in the context. The CJEU recognizes the differences between the internal and external settings by acknowledging minimum guarantees of the data that have been transferred to third countries for the persons to have enforceable rights and sufficient protection of any abuse, and not to require the intelligence files to be reviewed by citizens of another country, like some authors may emphasize[83].

78 EDPB recommendation mentioned above (18 June 2021), page 4.

79 EDPB (2021), page 4.

80 EDPB (2021), page 38.

81 Tzanou, Maria, (2020), page 17.

82 Milanovic, Marko, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 56 Harvard International Law Journal 81, 132, 2015.

83 Swire, Peter, '"Schrems II" backs the European legal regime into a corner — How can it get out?", International Association of Privacy Professionals (IAPP), 2020. Available at: <https://iapp.org /news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/>

Anyhow, although the Court's tried to be flexible in the extraterritorial context and giving solutions, and obligations, to companies and estates to manage international data transfers to European Union countries, there are challenges remaining that make the future of this vital matter uncertain.

3.4 The challenges of Schrems II and the future of "trans-data"

The *Schrems I* case demonstrated that the European Union was not successful in guaranteeing the fundamental right to the protection of personal data nor the adequacy procedure or appropriate safeguards serving no purpose when the data subjects live in an illusion that they are being protected[84] when the personal data is being transferred to third countries where surveillance programmes with not enough safeguards for the ones that are being supervised.

Schrems II was an evolution. It presented a more robust internal, and not that robust, external approach to extraterritoriality bringing legal certainty and clarity of the applicability of EU law and the merits of assessing external interference with EU fundamental rights but also, with the help of EDPB, presented to the relevant parts affected that there are ways to maintain the transatlantic market operating, with risk mitigation from additional protective measures. The achievements that were brought to the case were achieved indirectly with the highlight of something that is not in the article 44. and 45. of the GDPR, the concept of *risk assessment*, a development of the concept of *accountability*, because the entities need to be accountable, responsible, for what they do.

But even if it evolved, it was not the metamorphosis that was necessary, and here is why: the Court opened the discussion of how we can develop the steps to allow us to process data internationally in the future but didn't say that we needed something new compared to the last decision; the GDPR and Directive do not solve the issue in this case, because, even with all the efforts made by the companies that are following the recommendations, third parties are still able to perform these type of things, continuing to be illusory for the data subjects; increased burdens for both data controllers that transfer data and

84 Moniz, Maria da Graça, 2018, page 289 and 290.

the parties in third countries that received them[85]; and also third countries have in place regulation that allows data surveillance and European regulation that *per si* cannot solve this.

Technology can help find solutions, but before we get too inventive, we need to be reminded of the limitations that some emerging ones has, like *Blockchain*. Having the data being stored in a digital ledger that makes it hard to find, affects the rights of data subjects, but we also have a regulatory issue, because companies that have their headquarters in specific countries are forced to collaborate with authorities of their countries, even if they are providers of a technology that ensures that they do not have access to data, by law they are forbidden for having that solution, legal problems that are involved in this can be found in the Microsoft case[86]. Even if we have the technology that can solve this problem, finding an international middle term between the many legislators in the whole world about the way to transfer data in a safe and respectable way seems utopian.

In my opinion, the GDPR will not lead in, and to massive changes in the field of international data transfers for the EU to give the next relevant step. Considering that, we require other fields we need to focus on the role of additional technical protection measures, focusing on cybersecurity tools, that can help organisations using SCCs, main tool for data transfers, to provide the European level of protection when the data is flowing the world and possibly subject to public surveillance[87]. These measures include: the use of robust end-to-end encryption with one or more independent EU/EEA-based trustees securely holding the keys, and multi-party homomorphic encryption,[88] that

85 Kuner, Christopher, 2020.

86 United States District Court for The District of Columbia, United States of America V. Microsoft Corporation (5 November 1999). Available at: <https://www.justice.go v/sites/default/fil es/atr/legacy/2006/04/11/msjudge.pdf>

87 Compagnucci, Marcelo and Aboy, Mateo and Minssen, Timo, "Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)", page 11 and 12, 2021. Available at SSRN: <https://ssrn.com/abstract=3951085>

88 Marcelo Corrales Compagnucci and others, 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?', European Pharmaceutical Law Review 3(4):144-155. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3488291>

should be implemented within an overall ISMS[89] and PIMS[90] that is properly scoped and regulatory stress-tested, but also independently audited through third-party certification audits (ISO27001/27701).

In short, the Court of Justice of the European Union is serious about the fundamental rights dimension of data protection, but also finding a balanced way to maintain the foundations of Safe Harbour and the transatlantic data transfer, probably with an evolved international law, tons of established treaties, but we can assure that we are getting a lot of case law in the coming years and new challenges with technological and security advancements in the Digital Era.

4. Elgizouli V Secretary of State for The Home Department: a gap in the international data transfer framework?

4.1. Context

Exactly at 11 p.m. GMT, on January 31st, 2020, the UK ceased to be a Member State of the EU. In terms of its impact on the adoption of the EU legal framework, it left the UK with the Data Protection Act 2018 (DPA), adding to the GDPR where Member States were allowed to regulate, and combined it with regulation for processing activities outside the scope of the GDPR, being created to be in force at the time that the exit was finalised.[91] Post-Brexit European legislation was no longer in force. However, the regimes will be shown to be near-identical, with the UK mirroring the European approach to data protection, namely in international data transfer.

4.2. The Case

Shafee El Sheikh, a former British citizen, was accused, in the USA, of being involved in terrorist activities and the murders of several US and British citizens. This happened due to links Mr El Sheikh shared with a terrorist

89 Information Security Management System (ISO 27001).

90 Privacy Information Management System (ISO 27701).

91 Celeste, Edoardo, Cross-Border Data Protection After Brexit, Brexit Institute, Brexit Institute Working Paper Series, No 4/2021, 2021, p.5. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784811>

organization based in Syria, acting in the context of the civil war.[92] The crimes listed bore special gruesomeness.[93]

On June 22nd, 2018, the SSHD[94] of the UK Government at the time, decided to grant a request made by the Government of the USA, under the MLA,[95] pursuant to this case. The request materially involved the sharing of personal data of the individuals identified by the US Government. Due to the grave nature of the crimes, and the permissibility of employing capital punishment as a penalty for crimes of this legal type within the US legal framework,[96] the SSHD sought guarantees about the avoidance of the death penalty in this particular case. The US DoJ[97] only assured that they would "introduce no evidence obtained in response to this request in a proceeding against any person for an offence subject to the death penalty. In the event that the evidence was to be introduced, the United States would take the decision not to seek the death penalty, a decision which in the federal system absolutely precludes the death penalty from being imposed.",[98] known as a "Direct Use" undertaking. This would not prevent the influence of the evidence provided by the SSHD in informing the investigation and could make it practically part of the chain of conduct that would lead to an eventual death penalty sentence. The information was later shown to US investigators merely on an "information-sharing basis" in February 2018.[99]

In January 2018 Mr El Sheikh was taken into custody, providing the beginning of legal and eventual court proceedings. The conversations between the US Attorney General, the SSHD and Security Minister for the UK began.

92 Why has the Syrian war lasted 10 years?, BBC News, 2021. Available at: <https://www.bbc.com/news/world-middle-east-35806229>

93 [EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, The History, 5. and 6. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

94 Secretary of State for the Home Department.

95 1994 Treaty of Mutual Legal Assistance in Criminal Matters between the US and the UK.

96 "PATRIOT ACT II" PROVISIONS IN H.R. 10 (AS PASSED BY HOUSE), ACLU. Available at: <https://www.aclu.org/other/patriot-act-ii-provisions-hr-10-passed-house>

97 United States Department of Justice.

98 EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, 8. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

99 Ibid. 12.

The UK decided not to try Mr El Sheikh, due to lack of evidence and sought to support the US in their attempt. Eventually, the cabinet of SSHD was succeeded and its new holder had a more favourable outlook on whether the death penalty should act as a deterrent to the acceptance of the request. Adding to this, the UK Ambassador in the US recognized the tension and that the need for assurance to not seek the death penalty might deter the US from prosecuting Mr El Sheikh and perhaps lead to his confinement to the Guantánamo Bay Detention Camp.[100] The SSHD maintained their fear of the strong contemporaneous political tensions regarding this matter and their concerns as to Mr El Sheikh's confinement to Guantánamo being a result. This culminated in the granting of the request by the SSHD in a letter to the US Attorney General in a letter, with a mention as to how "there are strong reasons for not requiring a death penalty assurance in this specific case, so no such assurances will be sought".[101]

Mr El Sheikh's mother, Ms El Gizouli, was the claimant in this case. She submitted her request, speaking on the effect the decision had on her, and also challenging its merits. She sought to declare the decision made was unlawful, set a precedent preventing the absence of said assurance, an order that forced the SSHD to secure the destruction or return of the data and demand and an assurance as to Guantánamo Bay.

A) The Ground

The initial complaint was submitted on several grounds, among which are: the illegality and breach of the rule of law, that the exception to the policy is inconsistent with its rationale, errors of law disclosed in the decision letter, the violation of the claimant's Convention rights and the unlawful transfer of personal data in breach of domestic and EU data protection law. For this work, it is of particular relevance to analyse the unlawful transfer of personal data in breach of domestic and EU data protection law. The data transfer in question took place a month after most of the DPA came into force. Seen as

100 Guantánamo Bay Detention Camp, ACLU. Available at: <https://www.aclu.org/issues/national-security/detention/guantanamo-bay-detention-camp>

101 EWHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha El Gizouli) And The Secretary Of State For The Home Department, 2019, 8. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

that this is a criminal investigation, aiming to originate criminal charges, and this information in question relates to that, it is inevitable that it qualifies as personal data, per the definition of both the DPA[102] and the GDPR.[103] It also doesn't qualify as personal data regulated under the GDPR scope as per the DPA[104] and GDPR[105] definitions, being that the data is being processed for criminal procedure purposes. It is abridged by Section 3 of the DPA, which is dedicated to the processing of personal data by the authorities competent to investigate criminal matters, as well as Directive 2016/680 of the EU,[106] also known as the Police Directive[107]. Their definitions of personal data still apply in spite of the different matter, maintaining the harmony that was aimed at during the big legislative efforts around the protection of said personal data.[108]

As article 29 of the DPA indicates, the following articles apply to the processing of the personal data category we previously mentioned by a competent authority, as defined by article 30 (1) (a) and Schedule 7, as well as a controller, as defined in article 32. In that way, the SSHD is subjected to this legislation and therefore, the legal demands for international data transfer considerations. The claim alleges that this is matter is international data transfer abridged by the law stated above and is in breach of sections 35 (lawful and fair data transfer demands) and 36 (the collection of data must be specified,

102 Data Protection Act 2018, Article 2 (1).

103 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 4(1).

104 Data Protection Act 2018, Article 29.

105 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital (19) and Article 2 (2) (d).

106 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

107 European Data Protection Supervisor, Police Directive. Available at: <https://edps.europa.eu/data-protection/our-work/subjects/police-directive_en>

108 Edgar, Michael, *Harmonising European data protection law Agreement reached on the General Data Protection Regulation*, Laytons Solicitors. Available at: <https://static1.squarespace.com/static/570665c1 d51cd45f7c8f1812/t/5824c62cf7e0ab32fa764efc/1478805039099/Harmonising+European+data+protection+law+Focus+Jan+2016.pdf>

explicit and legitimate, and the manner of collection can't be incompatible with the purpose of the collection), as well as the specific sections 73 to 76, the specific data transfer section, defining its general principles. These are complex principles, demanding 3 conditions be met in order to be fulfilled subsidiarily in the following order: adequacy, appropriate safeguards and special circumstances. There is a correlation with the Police Directive, with article 4 (1)(c), requiring adequacy, which is materialised in recital, and article 35 (1)(d) that establishes this subsidiarity in the same order with the same concepts in mind. The articles in both the legal diplomas are almost mirrored, although slightly more concretely stated in the Police Directive. Article 36, referred to the adequacy decision, the consideration taken into account can be summed up to abidance with the law on the plain of human rights, public security, defense, national security and criminal law, the existence of a proper supervisory authority, and the obligations the other party to the transfer has entered into. Articles 37 and 38, relating to the appropriate safeguards are practically identical to their equivalents in content and language. There are also special restrictions for the processing of the data in section 80 of the DPA regarding the application of the international data transfer section, ensuring that when faced with international data transfer, the restrictions applied for national data transfer are also transposed and enforced.

As we have seen before, there was no consideration of these matters of the law in the initial decision, which focused on the penal side.

B) The decision

The Court[109] decided against the claimant in this matter.

The data protection part of the claim begins by annulling the argument of the unfairness of the decision by way of interpretation of the concept as meaning material transparency with the data subject about the use of their data, moving on to the lawfulness criteria, that is set aside due to the court's understanding that the record-keeping needs not to be a "bespoke set of documents",[110] rendering the claimant's argument as lacking merit, and finally

109 England and Wales High Court (Administrative Court)

110 WHC 60 (Admin) Case No: CO/3449/2018, The Queen (on the application of Maha

that the argument for special circumstances, due to the claimant's classification of this matter as "sensitive processing", revealing to be a difficult matter for the court to assess due to not having actual possession of the information to be able to discern whether it contains "racial or ethnic origin, political opinions, religious or philosophical beliefs",[111] resulting in a rejection of claims regarding the First Data Protection Principle of the DPA.

The Second Data Protection Principle claims were equally dismissed in the context of the court considering the intent to aid in a foreign prosecution was probably there from the start of the investigation, when the evidence was being collected, and that the means were proportionate.

The part of the claim regarding the transfer of personal data to a third country follows the same path of dismissal through the court considering every condition to be met and that the requirements are not necessarily expressly regarded, rather than the substantive reality secures the appropriate safeguards, excusing the SSHD as a consequence of considering they duly evaluated all possibilities, and the solution was necessary.

Lastly, with regards to the special processing restrictions, the claim was dismissed by way of considering that the section at hand cannot be subjected to the use as a way to manipulate a third country's sentencing law and shouldn't be a deterrent from applying to the MLA.

The appeal resulted in a similar outcome.[112]

4.3. European Law considerations

As we have been able to gather, Brexit impacted the application of European law in the UK. The final Brexit agreement provided that the UK would become one of the non-member-state countries with the closest framework in the area of data protection to the EU framework. Due to their

---

El Gizouli) And The Secretary Of State For The Home Department, 2019, 189. Available at: <https://www.bailii.org/ew/cases/EWHC/Admin/2019/60.html>

111 Ibid. 191.

112 EWHC 2516 (Admin) Case No: CO/3082/2020, The Queen (On Application Of Maha Elgizouli) And The Secretary Of State For The Home Department And Director Of Public Prosecutions, 2020, 65. Available at: <https://www.judiciary.uk/ wp-content/uploads/2020/09/ Elgizouli-v-SoS-Judgment.pdf>

five-decade long presence in the EU and the consequent adoption of all its directives, the aforementioned DPA, the national transposition of the Data Protection Directives[113] and the UK GDPR all reflect the European legal vision.

The Police Directive shows itself as the EU's attempt to bring forth international cooperation on data protection and international criminal prosecution.[114] It also shows itself as not an attempt to interfere with other countries' legal frameworks, imposing the European boundaries onto other countries which have different views on the definition of criminal types.[115] There is still the question regarding the possibility of the death penalty, the one that arose. There is a lot of legal discourse around whether the death penalty is a violation of human rights.[116] Article 2 of the EUCFR states in its article 2(2) that no person may be sentenced to the death penalty or executed. This is legislation that applies to European space. However, it is essentially a list of the values the union upholds above all and the question arises: even if in regards to a third country that supports this that would be considered a cruel and unusual punishment in the European space, should we override the principles of international cooperation, non-interference with external law application, and the basic layout defined by the data protection framework, when contributing to possible employment of the death penalty?

The truth is that this is a complicated matter. Lord Kerr, the dissenting justice in the appeal, marked a strong opinion against allowing the contribution of the UK to a possible death penalty, enhancing how the common law has not yet evolved in this matter, even though it is custom that the UK Government

113 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 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

114 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Recital (7).

115 Ibid. Recital (14)

116 Charter of Fundamental Rights of the European Union. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=PT>

rejects any employment of the death penalty, and the UK, as well as European countries, do not perform extraditions, deportations and other transfers of people without assurance.[117] It would seem coherent and also withhold evidence without assurances, given the extreme importance of safeguarding lives. Besides that, as Lord Kerr points out, the law is ever evolving and meant to reflect the morals and values of the contemporaneous society. With an ever-growing number of countries joining the abolitionist group, more than doubling between 1991 and 2017,[118] reflecting the undeniable majority of countries in the world, it is not only logical according to the framing of the legal provisions, but also reflective of the ideals shared among the world that life should trump any other interest at stake.

4.4. Should the "Police Directive" be adapted?

Data protection has become a very demanding and pressing question in the digital age. The rise in technology provided the ability to store, process and use unprecedented amounts of data for any purpose imaginable. This has also begun taking a toll on individuals. That is the context for the emergence of regulations such as the Police Directive. Would it make sense, given the circumstances of this case and the very real possibilities that it may reoccur, to alter the data protection directive that resolves this matter?

In its recitals, the Directive informs on how its conception can be associated with the increased technological advancements and the insecurities that follow them.[119] Criminal Authorities can now store that more data and the process becomes increasingly less transparent to the data subject, that does not necessarily have the capabilities to screen. This Directive was created for

117 Human Rights Committee, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30. Available at: <https:// tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/CCPR_C_GC_36_8785_E.pdf>

118 *Death penalty: How many countries still have it?*, BBC News, 2020. Available at: <https://www.bbc.co m/news/world-45835584>

119 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Recital (3)

that reason, to ensure that every individual is duly protected from the parties holding the power: in this case, the competent authorities. Whether it be a data protection authority, the criminal authority, or any branch of the government, these institutions may not be the most transparent when not needed, in order to facilitate the accomplishment of their goals. Ensuring that all the international data transfer is subjected to a final threshold of passing the non-facilitating test,[120] perhaps inside the sequence established in article 35, safeguarding that in any case that capital punishment is at play, the obligation to obtain assurance. Or perhaps the next occurrence of a similar case will be within the EU Member-States and may be appealed all the way up to becoming European case law with some force and incentivize the law to be interpreted in that way.

4.5. Data Governance as a means of intimidation?

The final question regards the potential to use this gap in the law that allows European nations to tacitly condone the death penalty by way of inaction is the lack of legal certainty. It is in fact customary for these types of international data exchanges to come accompanied with assurances, as the UK has this as the bastion of case law on the matter. However, with a precedent of admissibility of interpretation, and in spite of Brexit, we now have a clear avenue that governments can use to take advantage of the delay of other countries in matters of death penalty abolition for political gains.

This particular matter was decided due to heavy political tension and many moments of attempted negotiation, but the result was the lack of protection of a person's right to life that the UK was in a position to assure. Can wars begin to be waged by these means? Can countries effectively begin to use international cases and hold data hostage to bargain for political envisionments of the result? A reality in which the sharing of personal data is decided through political manoeuvring may result in countries outside the EU leveraging commercial benefits, economic partnerships and other political liaisons to pressure European Governments into conceding on matters of this regard. The

120 Based on the *"non-facilitation argument"*, Hilary Term [2020] UKSC 10 On appeal from: [2019] EWHC 60 (Admin), 68. Available at: <https://www.supremecourt.uk/cases/docs/uksc-2019-0057 -judgment.pdf>

SSHD was not entirely resistant to the idea at the moment of taking office. They were nevertheless bent to the will of the US Attorney and Government, who were threatening to possibly subject Mr El Sheikh to an almost certainly worse fate being held in Guantánamo. The SSHD bent to that will due to not having enough bargaining chips at the moment and having the decisions in their hands. The solution pointed to above to make a written declaration of legal obligation in the Police Directive would end the ability to negotiate and set the bargain in stone for states outside the EU that do allow for this type of punishment.

5. The Recent Case of the Russian Protesters and Portugal's Breach of the GDPR

5.1. Factual context

The GDPR is strongly committed to the protection of the rights recognized to individuals, not only concerning their data, but also the circumscribed fundamental rights, and although it applies mandatorily only in the countries of the European Union, it is not disconnected from the reality in which we live.

Today's globalized and digital society, which allows (and even "forces") us to be increasingly connected and seems to facilitate everyday processes, often reveals "the other side of the coin", bringing new challenges and problems and, with them, new dangers for individuals, who are increasingly exposed to possible violations of their rights, recognized and enshrined in various international texts.

That said, in this chapter will be analyzed a recent case, occurred in Portugal, where these issues will be addressed, in a critical way, and having the final goal of sketching directions for the future of the Union regarding specifically the issue of data transfers to third countries and the underlying relationship with fundamental rights.

The case began in January 2021 when the Lisbon Municipality breached the GDPR by illegally transferring the names, addresses, and contact details of three individuals who took part in a protest in Lisbon for the release of Alexey

Navalny, an opponent of Vladimir Putin's regime,[121]to the Russian Embassy, without any legal justification.

The Municipality did not seek to legitimize its actions, admitting that the transfer of the data in question was "inadequate".[122] As a "justification", it only pointed out the "lack of updating of bureaucratic procedures" related to the organization of demonstrations. According to CML, what happened was that, in compliance with Decree-Law 406/74 of 29 August, which regulates the right of assembly in Portugal, "«(...) the data of the three organizers was received" and that this information was "sent by CML's technical services to PSP/MAI and the entity/location of the demonstration (in this case, the Russian embassy of consular services), under the general procedure adopted for demonstrations »."."[123]

Thus, instead of informing only of the event, since it would take place in front of the Embassy, it advanced the personal data of the demonstrators, "(...) when the law does not expressly provide for the sending of this specific data".[124]

The National Commission for Data Protection (the Portuguese supervisory authority) has already opened an enquiry to ascertain the facts and the applicable consequences. However, since we do not have much information so far, this section will focus on a strictly academic analysis of what may be the implications in question.

5.2. Transfer of personal data to a third country

The extent of the concept of "data transfer" has been much debated in European doctrine and jurisprudence, as the GDPR has chosen not to expressly

121 Agência Lusa, *Comissão de Proteção de Dados abre inquérito a partilha de dados com a Rússia*, Observador, 2021. Available at: <https://observador.pt/2021/06/10/comissao-de-protecao-de-dad os-abre-inquerito-a-partilha-de-dados-com-a-russia/>

122 Ibid.

123 Lusa, *Câmara de Lisboa alterou os procedimentos de partilha de dados de manifestantes após caso Navalny*, Sapo, 2021. Available at: <https://www.sapo.pt/noticias/atualidade/camara-de-lisboa -alterou-procedimentos-de_60c1e615dba1497270e1df38>

124 Joana Petiz, *"Nada justifica a quebra da Proteção de Dados" e pode haver "responsabilidade criminal"*, Dinheiro Vivo, 2021. Available at: <https://www.dinheirovivo.pt/economia/nada-justifica-a-quebra-da-protecao-de-dados-e-pode-haver-responsabilidade-criminal-13828603.html>

adopt a definition.

When questioned, the European Commission departed from existing positions,[125] clarifying that "the term is often associated with an act of sending or transmitting personal data from one country to another, for example by sending paper or electronic documents containing personal data by post or email. Other situations that also fit this definition are all cases where there is an action of the controller to make personal data available to a third party located in a third country".[126]

This concept has also been discussed in case law, particularly in the *Lindqvist, Schrems* and *Schrems II* cases. However, with the indications of the Commission and the case law, we may conclude that in the present case we are dealing with a transfer of data, insofar it was an act of transmission of personal data, in electronic format, to a third country.

Concerning the definition of "third country", and although the Regulation once again does not specifically define what is to be understood by this concept, by recourse to Article 3 *a contrario sensu* GDPR we can extract that a third country is one that is not "situated in the territory of the Union". The European Commission has also clarified that a third country is a "country that is not a member of the EU".[127]

It is to be noted that the Embassies are a case of "extension of the application of national data protection legislation beyond national borders",[128] which means the Embassy is subject to Russian legislation, not the GDPR, even if located in Portugal.

Since Russia is not an EU Member State, it is considered a third country for the purposes of applying this Regulation, which requires an analysis of Chapter V, but also of the general rules and principles provided, first of all, in

125 Namely, the G29's position.

126 European Commission, "Frequently Asked Questions Relating To Transfers of Personal Data From the EU/EEA to Third Countries", 2009, cit., p. 18 via Moniz, Maria da Graça, 2018, pp. 242-243.

127 European Commission, "What rules apply if my organization transfers data outside the EU?". Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt>

128 G29, "Parecer 8/2010 sobre a lei aplicável", 16 de dezembro de 2010, cit., p. 30 via Moniz, Maria da Graça, 2018, p. 137.

Article 5, because although these data transfers are possible, it is necessary having in mind that "(the) protection granted by the Regulation (...) travels with the data, which means that the rules protecting personal data continue to apply regardless of where the data is located".[129]

As such, for data to be transferred from the EU, with the assurance that it will continue to have the same level of protection in a third country, certain conditions need to be met, as we will see below.

5.3. The absence of legal justification for the transfer of data

The GDPR dedicates its Chapter V and recitals 101 to 116 to the transfer of data to third countries, making it clear in article 44 GDPR that despite the intention to maintain the international relations in the field of personal data, this will only be possible if "(...) the conditions set out in this Chapter are respected by the controller (...)" and "(...) the level of protection of natural persons guaranteed by this Regulation is not undermined". To ensure such protection, the following articles underline conditions that must be met.

Firstly, Article 45(1) provides that "a transfer of personal data to a third country may take place where the Commission has decided that the country (...) ensures an adequate level of protection". After assessment of the level of protection, according to the criteria defined in the following paragraphs of the article in question, paragraph 8 dictates that "the Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries (...) which it has decided that an adequate level of protection is (...) ensured" and to which the Member States may transfer personal data.

From an analysis of the *Journal's website*, it appears that the Commission does not consider that Russia guarantees an adequate level of protection,[130] which means an EU Member State may not transfer data to that territory based on an "adequacy decision". In the present case, Portugal could not have sent the data on this basis.

---

129 Ibid.

130 European Commission, "Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection.". Available at: <https://ec.europa.eu/info/law/law-top ic/data-protection/international-dimension-data-protection/adequacy-decisions_pt>

Even if there is no such decision, article 46 GDPR presents another way to legitimise the sending of personal data to third countries, through its subjection to "appropriate safeguards" offered by the third country, and on the assumption that the data subjects enjoy "enforceable rights" and "effective legal remedies". The article also sets various means of providing these safeguards.

However, none of these predictions apply in this case, as CML sent the data without even being requested by Russia, which means this country did not present *a priori* any kind of adequate guarantees to justify the transfer.

Finally, article 49 cannot be resorted to either, since the situation in question does not fit the provision of any of its subparagraphs, not even in (d), which seeks to ground a transfer on "important reasons of public interest". A demonstration that has met the legal requirements and in the terms already described cannot, under any circumstances, fall within this criterion.

Furthermore, since that was a demonstration in favour of the release of an individual who has been imprisoned for opposing the regime of Vladimir Putin, even if the data sent appears to be content-neutral, it seems that we are, in reality, facing data revealing political opinions, considered a special category of data in Article 9 GDPR, whose processing is generally prohibited, and which makes the error committed by Portugal further compounded.

Although paragraph 2 presents exceptions to this prohibition, the concrete case does not seem to fit in any of the subparagraphs: it was not a legal obligation (paragraph b)), since the Portuguese decree on demonstrations does not impose the sharing of personal data of demonstrators; nor a transfer on public interest ground, since none of the requirements imposed by the subparagraph are met (*i.e.* the need for processing for reasons of public interest, the proportionality requirement, the respect for the essence of the right to the protection of personal data and the protection of the fundamental rights and interests of data subjects).

Finally, and as mentioned, although Chapter V enshrines the legal provisions regarding data transfers, the general principles and rules of the Regulation must be respected. Among these, we find lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability (article 5).

However, having arrived here, we have already concluded that CML, responsible for the data processing, has ignored both specific provisions of Chapter V and the general principles and rules of GDPR.

5.4. The fundamental rights at stake and remedies for right holders

As mentioned at the beginning of this chapter, the GDPR plays a pivotal role in protecting the rights of data subjects. Although instruments such as the Charter of Fundamental Rights of the European Union and the TFEU already ensure this same role, enshrining the right to the protection of personal data in their articles 8 and 16, respectively, the GDPR goes further. First of all, because it allows us to better understand the essence of this right in its recital 7, when it states that "natural persons should have control of their own personal", linking it to a "dynamic right" - the right to informational self-determination (*i.e.*, the right to control one's data).

However, it is necessary to be aware that there are other "concerns about the risks to fundamental rights arising from new processing of personal data triggered by technological development"[131] which go beyond the right to data protection in its strictest sense. It is now undeniable that "the processing of personal data poses risks to other fundamental rights",[132] which is immediately recognized by the GDPR, in its first article, and which lead authors to argue that this fundamental right, although autonomous from all the others, plays a role of "guarantee right"[133] by cherishing the protection of other fundamental rights, with which it has a "direct link".[134]

That said, it is now clear that the violation committed by the CML is even more serious than it might seem, as it is not just personal data as "simple data" that are at stake, but also what the disregard for this right means for the "dignity of the human person, freedom (of action, expression, thought),

131 Moniz, Maria da Graça, 2018, p. 67.

132 Mañas, José Piñar, "Objeto del reglamento", J. Piñar Mañas, *Reglamento General,* cit., p. 56 e ss. via MONIZ, Maria da Graça, 2018, p. 72.

133 Moniz, Maria da Graça, 2018, p. 72.

134 Calvão, Filipa, "Direito da Proteção de Dados Pessoais", Universidade Católica, Lisboa, 2018, cit., p. 51 via Moniz, Maria da Graça, 2018, p. 72.

autonomy, self-determination, personal identity, social participation"[135] and privacy of the three protesters.

Regarding remedies, data subjects in these circumstances are entitled to complain to a supervisory authority, by application of article 77 GDPR. In Portugal, the supervisory authority is the CNPD, as stated in article 3 of the Law No. 58/2019. In the present case, this complaint has been properly carried out.

In addition to this right, they can also take legal action against the controller, as provided in article 79. Once again, in the case under analysis, the protesters stated their intention to take the case to court against CML, mainly to prevent situations like this from happening again.

5.5. Accountability and other legal consequences

As regards the legal consequences for the Municipality, article 82 determines that if the existence of damages resulting from such breach is proven, it will be held liable and the three demonstrators will be entitled to compensation.

Furthermore, the Regulation provides for the imposition of fines due to its violation in article 83, which should be applied in the case under analysis. The amount will have to be determined by the NCDP according to the criteria set in paragraph 2. Paragraph 5 (c) further clarifies that the violation of the provisions on transfers of personal data according to articles 44 to 49 is subject to a fine of up to EUR 20 000 000. In this sense goes also Law No. 58/2019, in its articles 37 and 39.

Also, it is worth mentioning article 84 GDPR, which delegates to the Member States the establishment of other sanctions in addition to those already provided for in the Regulation.

---

135 Rouvroy, Antoinette e Poullet, Yves "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", Serge Gutwirth et *alii* (eds.), *Reinventing Data Protection?,* Springer, 2009, cit., p. 47 e ss.; Calvão, Filipa, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", Manuel A. VAZ *et alii, Jornadas nos quarenta anos da constituição da república portuguesa*, Universidade Católica, 2017, cit., p. 88 via Moniz, Maria da Graça, 2018, p. 72.

Therefore, article 46 of Law no. 58/2019 determines in paragraph 1 that "Whoever uses personal data in a manner incompatible with the determining purpose of the collection shall be punished by imprisonment of up to one year or a fine of up to 120 days". However, since we are dealing with the special data category of article 9, the penalty is doubled in its limits, as established in paragraph 2.

This diploma also determines in article 48 (1) that "whoever (...) transfers, for payment or free of charge, personal data without legal provision or consent, regardless of the purpose pursued, shall be punished with imprisonment of up to 1 year or with a fine of up to 120 days". Once again, the penalty is doubled in its limits since personal data referred to in article 9 is involved (paragraph 2). The identification of the concrete persons within CML responsible for the violation of the GDPR, who may suffer these penalties, will be verified during the enquiry already opened by the National Commission for Data Protection.

5.6. Final critique

The law is of little use if it only exists on paper. It needs to be respected. Although it enshrines ways to correct damage, the purpose of the law is to prevent such damage from happening, serving as a "guide" to action. And this goes for any law, whether it applies to individuals or legal entities, private or public sector.

However, since public entities are the authorities that run our country, it is unacceptable that they do not comply with the law, violating citizens' rights and even putting their lives at risk. It would be expected for their behaviour to serve as an example to their citizens, but unfortunately this is not the case.

As analyzed, Russia is not considered by the Commission to provide an adequate level of protection, nor is it a country known for respecting human rights (other than on paper). It indeed is one of the signatory countries to several international texts, in particular the Universal Declaration of Human Rights, but that does not mean the protection of rights exists in practice and not just on the formal level. This means that Portugal not only acted illegally, but also put the lives of three persons at risk.

In all these behaviours from State authorities, there is a common factor: the abuse of power concerning its citizens. It is vital to find ways to make sure that public authorities respect the law and not just subsequently accept the consequences that come from the abuses committed, since in such cases the damage to citizens will always be more severe than the consequences applied.

That said, and with the goal to maintain a climate of harmony between states and between public authorities and citizens, with respect for their fundamental rights, the EU shall always demand from Member States an outstanding behaviour *a priori* and, failing that, determine heavy consequences with a preventive function, in order to stop the abuses and actually protect individuals.

6. Conclusion

This work gives a broad overview of the many issues concerning the regulation of transborder data flows and raises some relevant questions in regards to future data protection possible alterations. Jurisdictions with different data privacy rules could cooperate to manage and facilitate the flows of data between them, and ensure national security and defense; corporations have an important role in international data transfers and cyberterrorism must be a matter of preoccupation.

Countries show a diversity of approaches to "trans-data" regulation, having as the main tension point the polarity of legal orders, like the EU's, that use the determination of *adequacy* of data protection in foreign jurisdictions as criteria, such as shown regarding the United States, and those that are more organizationally-based, using the *accountability* principle. This tension does not only regard data protection and privacy regulation, but of any regulation that is territorially-based, like most data protection and privacy law[136]. It is important to state that while regulation of capital flows and international trade has been liberalized in the last few decades, the regulation of transborder data

136 Kuner, Christopher, *Regulation of Transborder Data Flows Under Data Protection and Privacy L*aw: Past, Present, and Future (October 1, 2010). TILT Law & Technology Working Paper No. 016/2010, Tilburg Law School Research Paper No. 016/2010, page 39. Available at SSRN: <https://ssrn.com/abst ract=1689483≥

flows has been tightened, due, also, to the European acknowledgment that the data subjects are exposed to permissiveness of some countries so that their data processed for more purposes than should be required. Even with that it's not enough to find a common international port.

The only conclusion possible is that international data transfers give way to political tensions that are enhanced by the differences in criteria, especially with the crescent importance and popular attention paid to personal data related matters. It is imperative that these may be put aside, and a mostly harmonized legal order is incentivized to reduce conflict, block out political strategy, and focus on the protection of the party who this regime was created to protect: the natural person.