Chapter 92

International data transfer. An analysis of schrems cases I and II

https://doi.org/10.56238/devopinterscie-092

Maria Laura Grisi Sakamoto

1 INTRODUCTION

Addressing the current technology landscape, the internet, and the devices that are connected play a key role. Today's media open up a range of opportunities for man to present ideas, business, and forms of interaction[1]To make these interactions, we can understand that the transfer of countless amounts of data between one person and another is quite significant, so let us think about international data transfers and what their impacts on the world economy are. Here, the aim is to address the issue of international data transfer and discuss important decisions that directly interfere with the business made between the United States and the European Union, which also reflects on the global economy.

In a recent case of July 2020, called Schrems II, the Court of Justice of the European Union (CJEU) amended the understanding of the European Union Data Protection Commission (European Commission) on the international sharing of personal data between the United States and the European Union. The decision sought to elucidate some important points of transcontinental co-sharing of the data, such as: **(i)** whether the previously existing agreement, EU-US Privacy Shield, which authorized the transfer of personal data of individuals located in the European Union to the United States, met the requirements of the General Data Protection Regulation (GDPR); and whether **(ii)** the validity of the contractual provision the standard clauses approved by the European Commission are appropriate instruments appropriate enough for the international transfer of personal data.

The purpose of the Court of Justice of the European Union is to interpret European law to ensure that it is applied in the same way, uniformly between the countries of the European Union. It is a Community law that is deliberately dwelled on legal interpretations.

In a brief historical analysis, the Decision given in the Schrems II case comes from a series of rules and events already carried out between the European Union and the United States since 2000 with *the so-called Safe Harbour*, which the European Commission issued Decision No 2000/520/EC declaring that it

[1] FINKELSTEIN, Claudius. MALUF, Fernando. New Technologies and Constitutional Barriers to Economic Intervention by Public Administration.

provides adequate protection for EU data. However, with the Schrems I case, *the Safe Harbour program* was terminated in 2015, when denouncement was made by former U.S. National Security Agency (NSA) agent Edward Snowden over widespread privacy violations by the U.S. government, deeming the decision handed down in 2000 invalid.

In 2016, the 2016/1250/EC Dec isão was given, which created *the Privacy Shield*, enhancing the former *Safe Harbour*. The program required affiliated companies to guarantee certain rights to individuals whose data is transferred. With the GDPR in place, it has been discussed, as a subject of the Schrems II case, *whether the Privacy Shield program* would meet the requirements of the General Data Protection Regulation (GDPR).

In addition, the impacts of decisions on data transfers between the European Union and the United States may also affect Brazil, as *the Privacy Shield has been validated* as effective and compatible with the GDPR, ensuring adequate protection of personal data, the European Commission has set a precedent. In this sense, as the General Data Protection Law in Brazil was based on the European Regulation, with some minor variations, but, therefore, a high level of consistency with its devices, the effects generated concerning the GDPR can also be analyzed according LGPD.

2 BRIEF CONSIDERATIONS: PRIVACY AND DATA PROTECTION

Privacy is the individual concept of maintaining a private domain around us, of determining to what extent our thoughts, feelings, body, and identity is communicated to others. According to the Legal Encyclopedia of the Pontifical Catholic University of São Paulo (PUC-SP), personality rights are inherent to the man himself and aim to safeguard the dignity of the human person[2].

According to Carla Faralli, the right to privacy is an example, as Bobbio has said, rights have a historical foundation, that is, they are born and transformed in a way that corresponds with the moment of the historical condition are established, there may be, therefore, several meanings that change according to themselves historically in which it is, passing through the meaning of 'riservatezza' to the meaning of 'control of one's data' until the possible understanding of the identity of personal data.

The idea of intimacy began with Aristotle who already affirmed the existence of an intangible sphere of the individual to safeguard privacy with the notion of the public sphere and private sphere, in which he associated himself with family and private life[3]. We can, from form illustrative, for a better understanding of the idea of intimacy, recount the statement of Lord Chatham, who in 1766 made a pronouncement in the English Parliament on privacy and intimacy: "The poorest man challenges in his house all the crown, his

[2] HIRATA, Alessandro. Right to Privacy, Issue 1, April 2017. PUCSP Legal Encyclopedia. Available in: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade.
[3] RODOTÀ, Stefano

hut can be very fragile, his ceiling can tremble, the wind may blow between the ill-fitting doors, the storm can penetrate it, but the King of England cannot enter it.[4]"

Therefore, confirming Bobbio's thesis, which states that the law changes according to its historical context, intimacy and privacy were born as a moral essence and became a right in the legal sense, more today in the modern era.

2.1 EXHIBITION OF GENERATIONS OF DOCUMENTS THAT DEAL WITH INTIMACY AND PROTECTION OF PERSONAL DATA

Regarding the understanding of the right to intimacy and privacy, the following documents are presented: (i) Declaration of the Rights of Man and the Citizen of 1789; (ii) *The right to be alone*, 1888, by Thomas Cooley; (iii) *The right to privacy*, 1890, by Samuel Warren and Louis Brandeis; (iv) Universal Declaration of Human Rights of 1948; (v) 9th American International Conference of 1948[5]; (vi) the 1950 European Convention on Human Rights[6]; (vii) 1959 Pan-American Convention on Human Rights; (viii) *Freedom of Information Act Congress* of 1965[7]; (ix) Nordic Conference on the Right to Privacy 1967; (x)1981 Estrasburg Convention No. 108; (xi) Directive of the European Parliament and the Council (95/45/EC) of 1995; (xii) *Hessisches Datenschutzgesetz* from 1973[8]; (xii) Swedish Database Statute (Date *Lagen* 289 or *Datalog) of* 1973; (xiii) *Privacy Act North* America in1974; (xix) Federal Law of the Federal Republic of Germany - *Bundesdatenschutzgesetz* - on the protection of personal data of 1977; (xx) French Personal Data Protection Act - *Informatique et Libertés* - 1978; (xxi) Austrian Law - *Datenschutzgesetz (DSG)* - No. 565/1978; and (xxii) Decision of the German Constitutional Court - *Volkszählungsurteil* - 1983[9].

2.1.1 Brief analysis of generations of documents on intimacy and data protection.

Since 1789, countries have been creating laws and laws on the privacy and protection of personal data. From this collection of the documentation presented above, we can detect four generations of documents that we can identify from the given historical moment.

---

[4] FARALLI, Carla. GALGANO, Nadia Zorzi (the cure di), Persona and Mercato Dei Dati, South GdpR Riflessioni, 2019. Cit. p. 3 es.

[5] Article 5 - "Every person has the right to the protection of the law against abusive attacks on his or her honor, his reputation and his life air and familiar."

[6] Article 8 "Right to respect for life toilet and family. 1. Anyone has the right to respect his or her life toilet family, home, and correspondence. 2. There shall be no interference by the public authority in the of this right, but when such interference is Planned in law and constitute a measure that, in a democratic society, is necessary for national security, for public security, for the economic well-being of the country, the defense of the order and the prevention of criminal offenses, the protection of health or morals, or the protection of the rights and freedoms of others."

[7] United States Federal Law guarantees the right to obtain access to all personal information that is in the public domain.

[8] The law that an authority - *Datenschutz Beauftragen* (Commissioner for Data Protection) – would monitor the computer drawing of personal data in the confrontation with the public administration, in a pioneering initiative in Europe until then. Cf Vittorio Frosini. *Contributor i ad Un diritto Dell'informazione*. Napoli: Liguori. 1991, p. 191.

[9] This is Germany's most important data protection decision because it has set guidelines that have influenced the laws, doctrines, and case laws of several countries, such as Austria, Norway, and Finland.

The documents presented in the 1970s reflected the state of technology and the jurist's view at the time, which were marked by the conviction that fundamental rights and freedoms would be threatened by the unlimited collection of personal data, then carried out basically by the State. It is possible to identify, therefore, a balance of powers within the state, since it is primarily the Executive Branch that, with the use of personal data, would disproportionately increase its power of planning and control, about the other powers. Precisely for this reason, some laws of this first generation included instruments for the legislative power to have access to data[10].

The first generation continues until the *creation of the Bundesdatenschutzgesetz* (Federal Data Protection Law of the Federal Republic of Germany) in 1977 because first-generation data protection laws do not take long to become outdated due to the creation of a large number of data processing centers, which made it difficult to impose a control based on an authorization regime.

The second generation of these laws emerged in the second half of the 1970s and had as its first model the French law of 1978 (*Informatique et Libertés)*, which is characterized based on the consideration of privacy and the protection of personal data as a release of negative, that is, it gives the citizen the duty-power to protect and claim on their data, this change occurred given the dissatisfaction of people who suffered from the use of their data by third parties and lacked instruments to defend their interests directly.

The third generation began in the mid-1980s and began to cover more than the freedom of citizens to provide their data or not, but to effectively guarantee this freedom. It is from this guarantee that the fundamental direction of informational self-determination presented by the framework of data protection in German law, *Volkszahlungsurteil, is born*. Informative self-determination gives the individual the power to decide about the disclosure and use of his data[11]. Based on what Danilo Doneda exposes[12] "The laws of the third generation regarded the participation of the citizen as a driving force of its structure".

The fourth generation is the one we are currently, this generation seeks to meet the disadvantages of the individual approach previously existing and consists of the difficulty of basing the protection of personal data simply on individual choice. The fourth-generation laws seek to strengthen the position of the person about the entities that collect and process their data, recognizing the imbalance in this relationship, which was not resolved with measures that simply recognized the right to informative self-determination[13].

[10] AGRE, Philip; ROTENBERG, Marc. *Gendevelopment of data protection in Europe. Technology and privacy: The new landscape.* Cambridge: MIT Press, 1997, p. 224.
[11] MENKE, Fabiano. Data Protection and the Fundamental Right to Ensure the Confidentiality and Integrity of Technical Systemsinformational information in German law. RJLB, Year 5 (2019), No. 1.
[12] DONEDA, Danilo. From Privacy to The Protection of Personal Data. Thomson Reuters Brazil Content and Technology Ltda, 2nd Ed, 2020. Cit p. 178
[13] DONEDA, Danilo. From Privacy to Data Protection these are. Thomson Reuters Brazil Content and Technology Ltda, 2nd Ed, 2020. Cit p. 179.

2.2 EXPOSURE OF UNITED STATES LAW WITH THE PRIVACY AND PROTECTION OF PERSONAL DATA

Among the various *interpretations of privacy*, we can present three that are strongly present in the North American model: (i) the liberalist model, which considers data as goods, as *if they were new properties (commodities) that* are negotiable within a market; (ii) the transformation of data into *copyright-like rights,* which becomes the subject of exchange; and (iii) the guarantor model, which resembles the European data protection model, which treats the data based on the right to the person, with limitations and guarantees provided for in the planning.

The most striking characteristic that we can present in the North American data protection system is to be more liberal, that is, as stated earlier, it has market characteristics, being possible the freedom to negotiate this data in the market, that is, it interests *the United States informational privacy*, the *privacy linked* to the information economy[14] . The commercialization of data reduces settlement costs, advocates technological development, and allows individuals to obtain more services. The problem occurs in the acquisition of this data, and, therefore, there is a need to impose a controlled force that prevents offenses to companies and that can compensate for possible damages caused.

When it comes to the American model, we can understand that privacy is a constitutionally protected right implicitly, that is, the Supreme Court recognizes the right to privacy based on the 1st, 4th, and 14th amendments[15]. Based on what Danilo Doneda says[16] in his work:

> "The *right to privacy* has been or is evoked to regulate, among others, tranquility in the home itself, control over the body, control over one's own body, freedom of thought, control over surveillance, protection of reputation, protection against abusive investigations and interrogations, family planning, education of children themselves, abortion, euthanasia, among others."

The construction of privacy rights in the United States takes place from a *common law system*. Therefore, we can flag *the article The right to privacy has* led to a series of discussions on privacy in the país and is the most cited legal article in the history of the United States of America[17]. In 1905 the Georgia State Supreme Court accepted the views presented in the article and presented *the leading case of* the right

[14] STIGLER, Na Introduction to Privacy in Economics And Politics, The Journal of Legal Studies, The Law and Economics of Privacy, 1980, 9, 4, p. 263-644.

[15] Amendment I: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, OR abridging the freedom of speech, or f the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.
Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
Amendment XIV: All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.
Available in: https://www.law.cornell.edu/constitution/amendmentxiv <Access on 16.09.2021>

[16] DONEDA, Danilo. From Privacy to The Protection of Personal Data. Thomson Reuters Brazil Content and Technology Ltda, 2nd Ed, 2020. Cit p. 217.

[17] SHAPIRO, Fred. "The most-cited law articles revisited", in 71 Chicago-Kent Law Review 751 (1996).

to privacy: *Pavesich v. New England Life insurance*[18]. *The case of Olmstead v. United States*, in which the lawfulness of the interpretation of wiretaps engendered by the Federal Government without judicial authorization was cited *by the Right to Privacy by the United* States Supreme Court for the first time.

After this episode, the issue was also amply discussed by members of the Court, in which members Louis Brandeis and Oliver W. Holmes wrote *their Dissents* arguing that the Constitution should take into account the impact of modernization, in the sense that the Fourth Amendment will go far beyond the protection of property, of material assets that could be scoured, would be effective protection against intrusion into privacy by the government.

From what has already been presented, we can identify *that the right to privacy based on* the fourth amendment is what most identifies with the protection of personal data, being possible to observe, therefore, the existence of secrecy and isolation, the protection of a personal nature and a structure that comprises personal data. However, we can also identify other forms of privacy, which are directly linked to the First Amendment, ensuring freedom of expression.

In addition to this information that has been submitted, *we may also present the right to privacy existing in Tort Law*, which is a *Common law institute* that allows a person to obtain compensation for acts committed by third parties outside of a contractual relationship, and therefore *the erga omnes effect on decisions submitted* in a contractual relationship. This time, from the study presented above by Warren and Brandeis, we can list four *different torts in* the matter of the right to privacy:

> "1. *Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;*
> *2. Public disclosure of embarrassing private facts about the plaintiff;*
> *3. Publicity which places the plaintiff in a false light in the public eye;*
> *4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness"*[19]

It is possible to conclude, from the premises presented, that *the constitutional right to privacy* can only be charged for offenses committed, to some degree, by the State, leaving *to tort law* the cases between private individuals[20]. We can also set out the various state laws in the United States of America that deal with privacy and data protection.

Making a chronological analysis, the North American legislation on the subject is centuries-old, beginning in 1903 in the states of Virginia and Utah with the use of someone's name or image for commercial purposes without consent[21]. In the 1970s, federal laws on the subject were presented with the *Data Center*, *the Fair Information Practices Principles*, and the *Fair Credit Reporting Act* (FCRA).[22]" In 1974, the first U.S. law with the appearance of a general data protection law appeared, it is *the Privacy*

[18] 122 Ga. 190, 50 S.E. 68 (1905)
[19] PROSSER William. "*Privacy*", cit., p. 389.
[20] DONEDA, Danilo. From Privacy to The Protection of Personal Data. Thomson Reuters Brazil Content and Technology Ltda, 2nd Ed, 2020. Cit p. 238.
[21] *Misappropriation.* SMITH, Robert Ellis. *The law of privacy explained*, cit., p. 12.
[22] 15 U.S.C, § 1681 - 1681 That lei generated great influence in Brazilian legislation on the matter years later, based on what presents by Antônio Hermann Benjamin in Code Brazilian Consumer Protection Commented by the Authors of the Preliminary Project, 5th. Ed., Rio de Janeiro: Univer Forensics1997, p. 327

Act[23] and has limited effectiveness for federal agencies regarding the data that is stored by citizens. In 1986, *the Freedom of Information Reform Act was enacted to* ensure public safety; after, in 1996, the *Freedom of Information Act Amendments were published*, which addressed the theme of network communication technology. We can recognize that many laws have been emerging in the U.S. states that have been about *privacy.*

2.3 EXPOSURE TO EUROPEAN UNION LAW WITH PRIVACY AND DATA PROTECTION

Privacy is born as a right to isolate itself and to have no external interference, as presented above, as a right of "*riservatezza"*, and, as a result of this right and technological advances, the right to be only transformed into the right to the protection of personal data. In the European Union, the first provision for the introduction of data protection rules, following in the footsteps of Strasbourg Convention No 108, given in 1981, was the Directive of the European Parliament and the Council of 1995 (95/46/EC) which established the principle that the processing of data is legitimate if the consent of the individual is provided.

In line with the chronological understanding of the laws on data protection and digital law, we have Legislative Decree No. 196 of 30 June 2003[24], known as the Privacy Code, recognizing that privacy is an autonomous right to protection and personal, later confirmed by the Charter of Fundamental Rights of the European Union, which took place in the period 2000 to 2009 by the Treaty of Nice of 2001, and was linked to the Lisbon Treaty of 2009. The chapter on the right to freedom is explicitly the birth of the right to protection of personal data:

> "Ogni individual há diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere secondo il principio di lealtà per finalità determinate e in base al consenso della persona interessata o per altro fondamento legittimo previsto dalla legge. Ogni individuo há il diritto di accedere ai dati raccolti che lo riguardano e di ottenere la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".[25]

In 2016 the new European regulation on the protection of individuals with protection in the processing of personal data was given, which is Reg. (EU) 2016/679[26]. The difference between the European Data Protection Regulation (GDPR) of the Directive is that Dir. 46/95/EC has established,

---

[23] 5 U.S.C. §552.

[24] Legislative Decree 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella *Gazzetta Ufficiale* n. 174 del 29 luglio 2003 – Supplemento Ordinario n. 123. Available in: < https://www.camera.it/parlam/leggi/deleghe/03196dl.htm> Access on 21/10/2021.

[25] Charter of Fundamental Rights of the European Union - *European Union Agency for Fundamental Rights* - Official Journal of the European Union C 303/17 - 14.12.2017.
"Article 8 - Protection of Personal Data.
1. Everyone has the right to the protection of data from personal training that concerns them.
2. Such data shall be processed legally for specific purposes and with the consent of the person concerned or on another legitimate basis provided for by law. Everyone has the right to access the data collected concerning them and to obtain their rectification.
3. Compliance with these rules shall be subject to review by an independent authority."
Available in: https://fra.europa.eu/pt/eu-charter/article/8-proteccao-de-dados-pessoais. Accessed on 10/21/2021.

[26] *Regulation (EU) 2016/679 of the European Parliament and of the Council*. 27 April 2016 - *On the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General DatRegulation).* Available in: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 10/22/2021.

harmonized, and promoted equality in the processing of personal data by the Member State, based on an authorization approach; Reg. (EU) 2016/679 is founded on the *principle of accountability*, i.e. it is the responsibility of the data processing data subject to demonstrate that it has adopted legal techniques for the protection of those of[27] . Under a view of domestic and international *privacy law*, personality law has internally the right of confidentiality, the right to the protection of personal data, and the right to personal identity

The principle of "*Accountability"* or "Accountability" is based on the understanding that "organizations must be responsible for implementing applicable privacy and data protection requirements and should be able to demonstrate their compliance capabilities.[28]" This principle was also incorporated by the General Data Protection Law (LGPD), provided for in Article 6, item X[29], called "accountability and accountability".

3 INTERNATIONAL DATA TRANSFER

Technological development requires major changes and since the Industrial Revolution technology has become a prominent place in social dynamics. In this sense, the dimension that the technological phenomenon assumed has become a reason for the social sciences, including law.

With this, we can understand that technology is a conditioning vector of society and its development creates relationships to be regulated by law. With the emergence of the Internet, the possibilities of communication have expanded significantly and caused a large number of privacy-related questions to arise because it can facilitate a more frequent interaction between people, elements that are at the center of privacy issues.

With the advent of new technologies, communication between countries has become much greater, not only communications but also the use of data and trade between countries. With this, as Danilo Doneda presents in his work: the international dimension of the discipline of protection of personal data deserves attention not only in terms of the delimitation of conditions for the processing of the cross-border flow of personal data but also for its implications for each order[30].

[27] *Innovazione Technological and valore Della Persona. Il diritto Alla protezione dei dati personali nel Regolamento EU 2016/679,* cura di CALIFANO and COLAPIETRO, Napoli, 2017, and FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

[28] BACEN 4658, data protection, Data Security, DPVM, GDPR, ISO 27001, ISO 27701, Data Protection Act, LGDP. February 27, 2020. Available in: https://leadcomm.com.br/2020/02/27/o-principio-da-accountability-na-protecao-de-dados/. Accessed 10/22/2021.

[29] "Article 6 Personal data processing activities shall comply with good faith and the following principles:
(...)
X – accountability and accountability: demonstration by the agent of the adoption of effective measures capable of proving compliance and compliance with the rules for the protection of personal data and, including, the effectiveness of such measures."

[30] DONEDA, Danilo. From privacy to data protection. Fundamentals of the General Data Protection Act. 2nd Ed. 2019. Thomson Reuters Brazil Content and Tecnologia Ltda. São Paulo- SP. P. 248-249.

3.1 STUDY OF CASES SCHREMS I AND SCHREMS II

Based on the work General Law for the Protection of Personal Data and its repercussions on Brazilian law[31] "The concern to be taken into account when processing personal data is not limited to the protection of privacy following the guidelines of the internal legal system, but also necessarily integrates the risks involved in the transfer international data", so there is a great need to regulate the processing of personal data beyond the State.

In a study conducted by Reinhard Ellger, it was demonstrated that flows beyond the limits of the State are mostly : (i) personnel departments; (ii) banks, insurance companies, credit card companies, and *bureaus*; (iii) *direct* marketing; (iv) airlines and other agents of the tourism industry; (v) companies with foreign customers; and (vi) public sector entities[32].

However, what is intended to be demonstrated here is the strong American characteristic for compliance with data protection laws so that its international flow in the commercial, social, and political sphere, etc. is possible. Therefore, due to the Isloch of the circulation of information, there was a need for effective protection of personal data in an international situation with the cohesive matter. In this sense, more than a decade ago there has been a debate about the existence of a trend toward the convergence of international data protection rules [33].

Another factor for the international projection of data protection is the need for harmonization between international rules that make it easier for the international flow of personal information. In this sense, the first international document emerges: *the* OECD Guidelines[34]. At a later stage, with a more balanced perspective and influenced by the Council of Europe, there was the emergence of Convention 108 of 1981, as one of the most relevant instruments involving the global data protection theme. The convention is a cross-cutting regulation that stipulates a governance regime for personal data protection issues, consisting of an international framework that has begun to pave the way for a potential global data protection structure[35]. It is worth noting that Brazil has been one of the observers of the international committee of the convention since 2018.

At another time, Directive 46/95/EC disciplined the transfer of data in third countries and should be obeyed by the Member States of the European Union, as followed by the GDPR after a few years. The establishment and a minimum level and protection of personal data, present throughout the EU space, is

[31] TEPEDINO, Gustavo, FRAZÃO, Ana and OLIVA, Milena Donato. General Law for the Protection of Personal Data and its repercussions on Brazilian law. 2nd Ed, 2020, Thomson Reuters Brasil Conteúdo e Tecnologia Ltda, São Paulo, SP.
[32] ELLGER, Reinhard. Der Datenschutz igrenzüberschreitenden m Datenverkehr. Berlin, Nomos Verlagsgesellschaft.
[33] BENNET, Colin, Regulating Privacy, Data Protection and public policy in Europe and The United States, Ithaca: Cornell University Press, 1992, pp. 116-152.
[34] OECD Responsabile Business Conduct. OECD Guidelines for Multinational Enterprises. Available in: https://www.oecd.org/daf/inv/mne/48004323.pdf. Consultation in: 20/10/2021.
[35] FACHINETTI, Aline Fuke and CAMARGO, Guilherme. Convention 108+: the data protection treaty and the relevance of the theme for Brazil. July 4, 2021. Available in: < https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados>. Consultation on: 20/10/2021.

the necessary precondition to enable a free flow of such data within two borders[36]. The GDPR, in article 45, uses the technique of denying, as a standard solution, the transfer of personal data from the European Union to third countries, unless that country has a system of protection of personal data that meets the required level of adequacy[37].

3.2 INTERNATIONAL DATA TRANSFER BETWEEN US AND EU

As more private companies began advancing their data processing databases to collect significant amounts of personal data for business purposes, initial public debates about governments' use of personal data have been ruminated for the private sector. On the other hand, the Legislative Framework of the United States exhaustively regulated the activities of the federal government, however, it did not reach the private sector, which is subject only to the sectoral laws that provided a model based on voluntary compliance and enforcement by the Courts.

Thus, we understand that in the United States, politics is based on the conception of the free market; furthermore, the resistance to regulation by U.S. private actors has been greatly mitigated by the most influential companies in the market, which in turn advocate self-regulation as an effective means for protecting individuals, we deal here with an economic-legal mentality and efficiency considerations, that is, we are dealing with an FTC (*Federal Trade Commission) model.* , being the main path to the application of data protection and privacy of u.S. States.

After the creation of the EU Directive in the mid-1990s, we had the *creation of the General Data Protection Regulation* - GDPR which, after its creation, only a very small number of countries were recognized as suitable for eu data protection law. Specifically, in the United States, this legislation has been seen as a dangerous p receter for enforcing government regulation of e-commerce.

Because of the requirement of legality, the adequacy has been questioned by numerous U.S. scholars under international law and the General Agreement on Trade in Trade(GATS), stating that the regulation restricts signatory states from imposing restrictions on international data flows to result in arbitrary or unjustified discrimination against the United States. Therefore, the European Union has been welcomed as a window into a political change in the United States.

Expectations of U.S. suitability with European criteria have met resistance from U.S. national corporate interests in its legislative process to the economic part of the liberal market. In this sense, just as European regulation was widely criticized by North American scholars, the form of self-regulation promoted internationally by the United States government and its corporate actors was also not accepted by Europeans.

[36] DONEDA, Danilo. From privacy to data protection. Fundamentals of the Ger Lawdata protection agency. 2nd Ed. 2019. Thomson Reuters Brasil Conteúdo e Tecnologia Ltda. São Paulo- SP.
[37] *Ditto.*

European regulations influenced the international data protection scenario, which resulted in a well-known case called *Schrems.* To better understand the historical evolution of the data protection agreements that have taken place between the Unid states of America and the European Union, we will make a brief historical analysis of the cases in which the data protection problem has focused until reaching the point be worked on in this monograph: the Case Schrems II.

Therefore, we begin by stating that Maximiliam Schrems is a famous Austrian activist in the international data protection community. What Schrems intended was to question the interference and protection of European citizens' data against surveillance mechanisms and interceptions of U.S. intelligence agencies, as revealed by Edward Snowden in 2013[38].

> "Former CIA technician Edward Snowden, 29, is accused of espionage for leaking classified security information from the United States and revealing in detail some of the surveillance programs the country uses to spy on the American population, using theservers of companies such as Google, Apple and Facebook – and several countries in Europe and Latin America."[39]

In the Case of Schrems I, Max ran a campaign requiring Facebook to transmit all the personal data he had about him, in which case (*Europand V. Facebook*) the data was made public and taken to the Data Protection Commissioner of Ireland, becoming a surveillance case in the United States[40]. The case was brought before the European Court because of differences between Irish and European law (Art. 8 of the Charter of Fundamental Rights of the European Union[41]). A decision of the Europ Commission was therefore questioned in which it had approved an agreement called *Safe Harbour*, which appropriated and allowed international data transfer.

The invalidation of *the Safe Harbour agreement* stemmed from the concrete[42] the case that Maximiliam Schrems, a user of the social network Facebook, has the unreached transfer of his data to the United States, where the government developed invasive surveillance practices through the requirement of opening such information by internet operating companies.

Max Schrems denounced the legal apparatus for the international transfer of data between the United States and the European Union, claiming that the level of adequacy between countries would not be enough to ensure the protection of the personal data of European holders.

---

[38] VENTRE, Giovanna and MORAES, Thiago. The Saga of Schrems and the data protection compliance programs in Brazil. October 1, 2020. Available in: < https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020>. Consultation on: 20/10/2021.

[39] G1. Steps into the case of Edward Snowden, who revealed U.S. espionage. March 2, 2013. Available in: < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>.

[40] Epic.org. *Electronic Privacy Information Center. Data Protection Commissioner v. Facebook & Max Schrems (CJEU)*. Available at: https://archive.epic.org/privacy/intl/dpc-v-facebook/cjeu/

[41] "Art. 8º Protection of personal data.
1. Everyone has the right to personal protection concerning them.
2. Such data shall be the object of a treatment legal for specific purposes and with the consent of the person concerned or on another legitimate basis provided for by law. Everyone has the right to access the data collected concerning them and to obtain its rectification.
3. Compliance with these rules shall be subject to review by an independent authority".

[42]

The Schrems II[43] Tracase specifically issues the transfer of personal data in a global communication system such as the Internet there is a huge amount of data transfer. The impacts of Schrems II are not limited to the invalidation of the *Privacy Shield*, as we shall see below. Initially, the Advocate General indicated that there was no reason for illegality in the general contractual clauses, but about *the Privacy Shield*, in this sense from the point of view of what is discussed is the transfer of data that is in a Facebook account to the United States and questions whether in the USA there is legislation that does not call into question the principles of protection existing in the European legislation (Arts. 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and Art. 64 of the GDPR).

The decision in Schrems II not only solidified the ECJ's push for data security, but also had a significant impact on the economy and transatlantic trade, data sharing structures within law enforcement, and international data transfer far beyond the United States. In the North American view, the decision given in Schrems II is about "prevarication"; "hypocrisy" or "European imperialism".

3.2.1 *Safe Harbour:*

Safe Harbour was an agreement established in 2000 when the European Commission issued a decision declaring adequate protection for EU data based on Directive 95/46/EC). It is, in this sense, a self-certification structure that allowed organizations to organize private actions to meet the requirements of the European Directive for international data transfers. Companies wishing to participate certify their compliance with a set of principles. The renewal of this agreement should be carried out annually.

The agreement called *Safe Harbour* signed by the European Union after numerous threats of economic retaliation were due to the *Schrems I case.* Safe *Harbour* guaranteed the Americans the possibility of continuing, unharmed, without a standard framework for the protection of personal data and[44] had as principles: (i) Transparency in the information of users; (ii) freedom to choose whether and what data may be disclosed to third parties; (iii) transparency in the transmission of information; (iv) security and security for data protection; (v) data integrity and limitation of purposes; (vi) possibility of correction, complementation or deletion of incorrect or harmful information; and (vii) effective protection. [45] However,

[43]Maximillian Schrems v. Data Protection Commissioner. Available in: < https://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=en>.

[44] RULE, James B. Privacy in peril: how we are sacrificing a fundamental right in exchange for security and convenience. Oxford: Oxford University Press. P. 135-139.

[45] *(i) Notice: Organizations must notify individuals about the purposes Is Which They collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to Which It discloses the information, and the choices and mean the organization offers for limiting its use and disclosure.*

(ii) Choice: Organizations must give individuals the opportunity to choose (opt-out) Whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, an affirmative or explicit (opt-in) choice must be given if tHe information is to be disclosed to a third party or used for a purpose Other Than its original purpose or the purpose authorized subsequently by the individual.

(iii) Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may

self-certification was flawed and there was little oversight.

The agreement was invalid in October 2015 by a decision of the Court of Justice of the European Union (CJUE) in Case C-362/14, recognizing the inadequacy of the U.S. data protection regime in the face of strong interference and grafted by the Government on personal data in surveillance activities, especially by intelligence such as *the National Security Agency* (NSA)[46] . From then on, in the case of transfers between the US and EU regions, other mechanisms foreseen in the DPD should be used. One of the possibilities also present in the current GDPR is standard contractual clauses approved by the *European Commission (Standard Contractual Clauses - SCC).*[47]"

Based on Rocco [48]panetta's claims, one of the reasons for safe harbor's *invalidation* was because the document applied only to the American companies that adopted it, with the consequence that public authorities could simply invoke the exigency of the data from the reference to "national security" to eliminate practical relevance and effectiveness, resulting in indiscriminate access and a violation of the principle of necessity, proportionality and purpose of treatment.

After the invasion of *Safe Harbour*, the European Authority's focus was on developing a new agreement, proposing the legal instrument necessary for the international transfer of secure data.

3.2.2 *Privacy Shield*:

However, the safe harbor's *invalidation was* not enough for Schrems. Shortly after the decision that determined the invalidation of the agreement, a new action was filed against the 2010 Decision, in which the EC created a standard contractual clause (SCC) for international transfers of data between European controllers and U.S. operators. The case also advanced to the CJUE and became known as Schrems II.

---

do so If it makes sure that the third party subscribes to the Safe Harbour principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such a third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
(iv) Access: Individuals must have access to personal information about them that no organization holds and be able to correct, amend, or Delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in The case in question, or where the rights of persons other than the individual would be violated.
(v) Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.
(vi) Data integrity: Personal information must be relevant for the purposes for Which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
(vii) Enforcement: To ensure compliance with the Safe Harbour principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures have been implemented; and (c) obligations to remedy problems arising to ensure compliance by the organization. Organizations that Fail to provide annual self-certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.
Safe Harbour Privacy Principles U.S. Department of Commerce, 2000.

[46] TEPEDINO, Gustavo, FRAZÃO, Ana and OLIVA, Milena Donato. General Law for the Protection of Personal Data and its repercussions on Brazilian law. 2nd Ed, 2020, Thomson Reuters Brasil Conteúdo e Tecnologia Ltda, São Paulo, SP. P. 628-629.

[47] VENTRE, Giovanna and MORAES, Thiago. The Saga of Schrems and the data protection compliance programs in Brazil. October 1, 2020. Available in: < https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020>. Consultation on: 20/10/2021.

[48] PANETTA, Rocco. Il Transfer All'estero dei Dati Personali, Persona and Mercato I gave Dati. Riflessioni south GDPR, the cure di GALGANO, Nacia Zorzi. Wolters Kluwer CEDAM, 2019. P. 364-365.

Standard contractual clauses are a contractual tool that has a qualified nature for lawful data transfer abroad. In the event of the contract, predefined by the European Commission, *the data importer* and the importer (*porter)* should therefore be limited to the agreed document. Therefore,s SCCs exist to be included in commercial agreements of a broader nature to regulate the security aspects of personal data.

In this sense, we believe that CCS is the most common method for transferring data abroad in the absence of an adequacy decision. However, its content rigidity makes implementation difficult for companies operating in different countries, given the need to implement the same security and guarantee measures in very heterogeneous contexts.

The Schrems II case has had a greater impact on the daily lives of companies that have international data transfer as their activity. The Court of Justice of the European Union has ruled that, even if the clauses cannot be used as a safeguard measure to ensure minimum standards of data security and protection, they are not obstacles and should be subject to an analysis of the practice and legislation of the countries of destination – contractual liability.

In this sense, the Schrems II case pointed to a need to create international data protection standards, looking at the system as a whole, the international mechanism on which different governments can be based for public security.

During the occurrence of Schrems II, a new agreement known as the EU-US *Privacy Shield was created.* This agreement has a more robust feature *than the old Safe Harbour*, establishing seven principles for the international transfer of data, which should be validated from a self-certification, in which a company conducted an internal compliance plan, registered an international arbitration to regulate any conflicts and published a notice of its suitability to *privacy shield*. Therefore, the new agreement came to fill a gap left by the previous one.

In addition to other regulations, only U.S. legal *entities subject to the jurisdiction of the Trade Commission* or Department of Transportation are eligible to participate in *the Privacy Shield* and are administered *by the U.S. International Trade Administration*. To agree, a U.S.-based organization must certify itself to the *Department of Online Commerce*; once the commitment is made, it becomes mandatory and may be executed under United States law.

However, while the new lawsuit filed by Max Schrems did not expressly mention *the Privacy Shield*, *the* agreement was also the subject of analysis by the European Court because, according to *the Director of Research of the International Association of Privacy Professionals* Caitlin Fennessy, there are at least three factors that create a connection between the decision and *the Privacy Shield agreement*[49]*:* (i) the use of SCCs is mentioned by the *Privacy Shield*; (ii) the agreement does not define specific mechanisms for validating transfers, which gives a "tacit sanction" to the use of SCCs; and (iii) the Supreme Court of Ireland, which referred the case to the CJUE, questioned the latter as to the relevance of the pact to the case

[49] FANNESSY, Caitlin. The Privacy Shield review and its potential to impact Schrems II. November 5, 2019. Available in: <https://iapp.org/news/a/the-privacy-shield-review-and-its-potential-to-impact-schrems-ii/;

presented in this paper.

After review, the European Court concluded that *the Privacy Shield* does not provide adequate protection to European citizens against the activities of U.S. intelligence agencies, as it does not guarantee data subjects mechanisms to appeal against those authorities. The evidence, coupled with the fact that the directive regulates the U.S. intelligence services, the PPD-28, authorizes the conduct of massive surveillance, results in extreme disproportionality that undermines the adequacy decision that gave validity to the EU-UAPrivacy Shield[50].

The Cases Schrems I and II highlight, in a few words, that the holder of personal data must be in control of his information and such control must be effectively exercised. The decisions reinforce the need to implement a privacy program that ensures that the holder can effectively exercise his or her rights.

What was questioned in the decision that invalidated *the Privacy Shield,* to the extent that by allowing a self-certification of North American companies, the clauses inserted generate a system of self-binding. Thus, the regulation of the matter in defense and security they are not in harmony with European legislation.

At the final moment of the discussion, the Court maintained the validity of the SCCs, however, it was understood that the standard contractual clauses could not be and be linked to the state intelligence authorities that are not part of the causes and cannot completely replace the laws that apply to the data importer in their country of origin. The standard contractual clauses, though, are still limited, i.e. whatever mechanism is used to transfer data, it must still ensure an adequate level of protection of personal data.

3.2.3 *Consequences of the Decision invalidating the Privacy Shield*:

With the Decision of the European Court, the question that remains is: **how can data be legally transferred from the EU to the US?** After a decision was handed down, the court did not impose a mandatory and widespread prohibition for the transfer of data, but merely invalidated the Privacy Shield decision and review the guarantees provided to individuals in the legal system of the United States of America. As a result, it can be noted that adequacy decisions are not the only mechanisms for the transfers of personal data to third countries (Article 45(3) [51]GDPR or adequate safeguards under Article 46 of[52] the GDPR).

---

[50] VENTRE, Giovanna and MORAES, Thiago. The Saga of Schrems and the data protection compliance programs in Brazil. October 1, 2020. Available in: < https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020>. Consultation on: 20/10/2021.

[51] Article 45(3) GDPR: Transfers based on an adequacy decision (...).**3.** After assessing the adequacy of the level of protection, the Commission may decide, through an implementing act, that a third country, a territory, or one or more specific sectors third country, or an international organization, guarantees an adequate level of protection in the implementation of paragraph 2 of this Article. The implementing act provides for a periodic evaluation procedure, at least every four years, which should take into account relevant developments in the third country or the international organization. The implementing act shall be the territorial and sectoral scope and, where appropriate, shall identify the supervisory authority or authorities referred to in paragraph 2(b) of this Article. That implementing act shall be adopted by the examination procedure referred to in Article 93(2).

[52] Article 46 GDPR. Transfers are subject to adequate guarantees. **1.** No decision has been taken per Article 45(3), processors or processors may transfer personal data to a third country or an international organization only if they have provided adequate safeguards, and provided that data subjects enjoy effective corrective legal measures. (...)

In 2022 the issue of privacy and security with the Privacy Shield was again put on the agenda. Therefore, on 25 March 2022, Commission President Ursula Von der Leyen and President Biden announced a "*Agreement in Principle" in the* new EU-US data-sharing system. Given the information presented, Max Schrems, on his[53] The "Noyb" page, presented that the *announcement of a political agreement without sound legislation causes more legal uncertainty. What occurs is pressure from the United States on the European Union due to the Ukraine War which has caused major political, economic, and trade balances in the EU*[54].

"*Today* (March 26, 2022), *we have reached an unprecedented agreement on the privacy and security of* new *citizens' data,"* Said Joe Biden after meeting with Ursula Von der Leyen, President of the European Commission, she said: "*The transatlantic partnership stands stronger than ever. In a world faced with the disorder, our city upholds fundamental values and rules that our citizens believe in. And we are determined to stand up against Russia's brutal war"*[55]

After six months of discussion, the *so-called "Agreement in Principle"*, JOe Biden signed the Executive Order that aims to respect the previous judgments of the European Court of Justice (CJEU) to overcome the difficulties existing due to the decision given in Schrems II. in its decision, the ECJ demanded (i) that U.S. surveillance be proportionate to Article 52 of the Charter of Fundamental Rights[56]; and (ii) that there be access to legal redress as required by ArtIGO 47[57] of the same legal framework; which does not appear to be the case under biden's Executive Order.

---

[53] Noyb: https://noyb.eu/en

[54] ROCHA, Agnes. Marx Schrems. "Privacy Hero" praises cancellation of sending Census data to the U.S. July 12, 2021. Available at <https://rr.sapo.pt/especial/mundo/2021/07/12/max-schrems-heroi-da-privacidade-elogia-cancelamento-de-envio-de-dados-dos-censos-para-os-eua/245548/>

[55]Twitter: "The transatlantic partnership is stronger than ever. In a world confronted with the disorder, our city upholds fundamental values and rules in which our citizens believe. And we're determined to face Russia's brutal war" on March 25, 2022. Available at <https://twitter.com/vonderleyen/status/1507286462064214043>

[56] Article 52 - scope and interpretation of rights and principles: 1. Any restriction on the exercise of the rights and freedoms recognized by this Charter shall be provided for by law and the essential content of those rights and freedoms. In compliance with the principle of proportionality, such restrictions may be introduced only if they are necessary and correspond to objectives of general interest recognized by Unior the need to protect the rights and freedoms of others. 2. The rights recognized by this Charter which are governed by provisions contained in the Treaties shall be exercised by the conditions and limits defined by them. 3. In where this Charter contains rights corresponding to the rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights are the same as those conferred by that Conventionntion. This provision does not prevent EU law from conferring wider protection. 4. To the extent that this Charter recognizes fundamental rights arising from the constitutional traditions common to the Member States, such rights shall be in harmony with these traditions. 5. The provisions of this Charter containing principles may be applied using legislative and executive acts taken by the institutions, bodies, and bodies of the Union and by acts of the Member States when they apply EU law in the exercise of their powers. They shall be invoked only before the court to interpret those acts and monitor their legality. 6. National laws and practices shall be fully taken into account as needed in this Charter. 7. The courts of the Union and the Member States shall take due account of notes to guide the interpretation of this Charter. Available at <https://fra.europa.eu/pt/eu-charter/article/52-ambito-e-interpretacao-dos-direitos-e-dos-principios>

[57] Article 47 - Right to action and an impartial tribunal: Any person whose rights and freedoms guaranteed by EU law have been infringed is entitled to action before a court following this Article. Everyone has the right to have his cause be julfair, publicly and within a reasonable time, by an independent and impartial tribunal previously established by law. Everyone can make himself counsel, defend and represent in court. Judi assistance is granted to those who do not have sufficient resources, to the extent that such assistance is necessary to ensure the effectiveness of access to justice. Available in: <https://fra.europa.eu/pt/eu-charter/article/47-direito-accao-e-um-tribunal-imparcial>

In the case of more specifically the Executive Order, announced on October 7, 2022, it is an internal directive of the President of the United States within the Federal Government, but it is not a law and introduces a series of additional safeguards and requirements to limit *access to the data of European citizens*, in addition to establishing appellation system to deal with complaints.

However, according to what was presented by the official activist Max Schrems in his network "Noyb", which is an NGO responsible for the fight and enforcement of the protection of citizens' data, the Order exec utive there area number of problems, such as: (i) it is not a law and can be easily annulled by another executive order. Such a weak legal construction is unlikely to satisfy the CJEU; (ii) from the U.S. point of view, Europeanshave no right to privacy, i.e. the Fourth Amendment guarantees this only to U.S. citizens, while anyone else can easily become the target of government surveillance activities; (iii) U.S. organizations operating in the European Union will not be subject to the GDPR, in other terms, under the decree they will not need a legal basis for data collection and will only provide an *opt-out mechanism for* anyone who wishes to refuse to share their shares. This will put EU companies at a serious disadvantage because they necessarily need to comply with the GDPR.

4 CONCLUSION

We can conclude this analysis we can understand that it is important to establish international standards for the protection of personal data on how governments can access the data for public security, criminal prosecution and other legitimate purposes. Para Bruno Bioni, in *Webinar* presented under the theme, it would be interesting to *create binding corporate rules* that, if validated by regulatory bodies, would create a kind of safe intra-organizational zone for data flow, an example of these companies would be if entities of the same economic group can exchange data with each other.

Based on what has been settledin this work, we can understand that there are numerous problems existing when it comes to international data transfer, especially when the transfer takes place in a country that does not have a robust law that seeksto protect people's data. Currently, in the U.S. no general, broad and robust legislation for the protection of personal data is applicable throughout the country, which ends up hindering the relationship of commerce and application users from outside the country.

Since the Decision of Schrems II, which effectively banned the transmission of data from the EU to the US, many European organizations have updated their technologies and methodologies to operate by the renewed legal landscape. In this sense, the routes most used outside the limitation or exclusion of the transfer and anonymization of data, i.e., technology companies in the United States are dependent on user identification and data transfer, limit the latter and remove data from personal information can help in solving the problem, however, there is always a price; if we configure Google Analytics according to GDPR standards, the tool loses much of its functionality; and the updating *of technology stacks* with active altern of the European Union, which with the advent of Schrems II, has created a market space for European

companies to provide business software and marketing hosted locally in the Union, these alternatives allow companies to move away from the problem of data transfer.

The new regulations presented mark an end to more than two years of turbulence, but will not reverse the course of time. Schrems II has irreversibly changed the way companies and legislators approach the issue of privacy and data transfer, and the proof of this is the existence of other updates to the legal landscape, such as the Digital Service Act and the Digital Market Act, resanding the relationship between Europe and Bi g Us Tech, while the ePrivacy regulation still in progress will detail the regulations for data collection and processing for the digital world; yet, according to a recent [58]the study, more than 70% of EU marketing executives and CEOs are convinced of the importance of respecting users' online privacy, in this sense almost half of respondents plan to replace *their current stack* with EU-based alternatives. Finally, we notice the changes in digital marketing and advertising, which are sectors that depend heavily on the transfer and processing of personal data. Its two main mechanisms, the IAB TCF2 and the Real Time Bidding system, are now in the crosshairs of legal NGOs and the outcome of these investigations willreshape the industry's work in the European Union.

Finally, based on what Max Schrems states in his Noyb communication system:

> "Now, where the US has issued its Executive Order, the European COmission will have to draft a so-called "adequacy-decision" under Article 45 of the GDPR. Once the draft decision is issued, the Commission must hear the European Data Protection Board (EDPB), but is not bound by its findings. In addition, the European Member States must be heard and could block the deal. This process can take a couple of months. However, even negative statements by the EDPB and Member States are not binding on the Commission. Once the decision is published, companies can rely on it when sending data to the US and users can challenge it via the national and European courts. This is not expected before spring of 2023, even when it was originally envisioned in fall of 2022"[59].

[58] Available at <https://landing.piwik.pro/gdpr-survey-2022/>

[59] SCHREMS, Max. New US Executive Order unlikely to satisfy EU law, October 07, 2022. "Now, where the U.S. has issued itsthe Executive Order, the European Commission will have to draw up a so-called "adequacy decision" according to Article 45 of the GDPR. Once the draft decision has been issued, the Commission shall hear the European Data Protection Council (EDPB), but is not bound by thetheir conclusions. In addition, European Member States should be heard and may block the agreement. This process can take a few months. However, even negative statements by the EDPB and the Member States are not binding on the Commission. Theyes that the decision is published, companies can rely on it when sending data to the US and users can challenge it in national and European courts. This is not expected before spring 2023, even when it was originally planned for the2022. Available at <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>

REFERENCES

GODOY, Bruna Michele Wozne. Privacy Shield EUA x Brasil: é possível? Ed. 2020, Editora Revista dos Tribunais.

GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. 1ª Ed. 2018. Editora Lumen Juris.

Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira

DONEDA, Danilo. Da Privacidade à Proteção de Dados. 2ª Ed. Editora Thomson Reuters - Revista dos Tribunais

Webinar PG Advogados | Privacy Shield e transferências internacionais de dados pessoais. Disponível em: https://youtu.be/W9bOV2qDZxs

What is EU-US PRIVACY SHIELD? What does EU-US PRIVACY SHIELD mean? EU-US PRIVACY SHIELD meaning. Disponível em: https://www.youtube.com/watch?v=XMS_0lQuQow

LGPD em Movimento [Transferência Internacional de Dados]. Disponível em: https://youtu.be/75d3zSrg3e0

QUARTA DIGITAL - LGPD: Transferência internacional de dados. Disponível em: https://www.youtube.com/watch?v=oVoIy0XhqLA

PROSSER, William. "*Privacy",* cit., p. 389.

Misappropriation. SMITH, Robert Ellis. The law of privacy explained, cit., p. 12.

SHAPIRO, Fred. "The most-cited law articles revisited", in: 71 Chicago-Kent Law Review 751 (1996).

STIGLER, Na Introduction to Privacy in Economics and Politics, The Journal of Legal Studies, The Law and Economics of Privacy, 1980, 9, 4, p. 263-644.

CORNELL, Law. https://www.law.cornell.edu/constitution/amendmentxiv <Acesso em 16.09.2021>

AGRE, Philip; ROTENBERG, Marc. *General Development of data protection in Europe. Technology and privacy: The new landscape.* Cambridge: MIT Press, 1997, p. 224.
MENKE, Fabiano. A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão. RJLB, Ano 5 (2019), nº 1.

FARALLI, Carla. GALGANO, Nadia Zorzi (a cura di), Persona e Mercato Dei Dati, Riflessioni sul GDPR, 2019. Cit. p. 3 e ss.

HIRATA, Alessandro. Direito à Privacidade, Edição 1, abril de 2017. PUCSP Enciclopédia Jurídica. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade.

VIEIRA, Victor Rodrigues Nascimento. Lei Geral de Proteção de Dados: Transferência Internacional de Dados Pessoais. Disponível em: < https://vieiravictor.jusbrasil.com.br/artigos/726523659/lei-geral-de-protecao-de-dados-transferencia-internacional-de-dados-pessoais>.

FINKELSTEIN, Claudio. FEDERIGHI, André Catta. CHOW, Beatriz Graziano. Uso de Dados Pessoais no Combate à COVID-19: Lições a partir da Experiência Internacional. Revista Brasileira de Inteligência Artificial e Direito, ISSN 2675-3156. Vol. 1. N. 1. Jan-abr. 2020.

VIOLA, Mario. Transferência de Dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Rio de Janeiro. Novembro, 2019.

Digital Single Market: Commission publishes guidance on free flow of non-personal data. Comissão Europeia. 2019. Disponível em: < https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_2749>.

FINKELSTEIN, Cláudio. MALUF, Fernando. Novas Tecnologias e as Barreiras Constitucionais à Intervenção Econômica pela Administração Pública.

STIGLER, An Introduction to Privacy in Economics and Politics, The Journal of Legal Studies, The Law and Economics of Privacy, 1980, 9, 4, p. 263-644.

Misappropriation. SMITH, Robert Ellis. The law of privacy explained, cit., p. 12.

Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento EU 2016/679, a cura di CALIFANO e COLAPIETRO, Napoli, 2017, e FINOCCHIARO, Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017.

BACEN 4658, data protection, Data Security, DPVM, GDPR, ISO 27001, ISO 27701, Lei de Proteção de Dados, LGDP. 27 de fevereiro de 2020. Disponível em: https://leadcomm.com.br/2020/02/27/o-principio-da-accountability-na-protecao-de-dados/. Acesso em 22/10/2021.

TEPEDINO, Gustavo, FRAZÃO, Ana e OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. 2ª Ed, 2020, Thomson Reuters Brasil Conteúdo e Tecnologia Ltda, São Paulo, SP.

ELLGER, Reinhard. Der Datenschutz im grenzüberschreitenden Datenverkehr. Berlin, Nomos Verlagsgesellschaft, 1990.

BENNET, Colin, Regulating Privacy, Data Protection and public policy in Europe and the United States, Ithaca: Cornell University Press, 1992, pp. 116-152.

OECD Responsabile Business Conduct. OECD Guidelines for Multinational Enterprises. Disponível em: https://www.oecd.org/daf/inv/mne/48004323.pdf. Consulta em: 20/10/2021.

FACHINETTI, Aline Funke; CAMARGO, Guilherme. Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil. 4 de julho de 2021. Disponível em: < https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados>.

VENTRE, Giovanna e MORAES, Thiago. A Saga de Schrems e os programas de conformidade à proteção de dados no Brasil. 01 de outubro de 2020. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020>.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. 02 de março de 2013. Disponível em: < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>.

Epic.org. Electronic Privacy Information Center. Data Protection Commissioner v. Facebook & Max Schrems (CJEU). Disponível em: https://archive.epic.org/privacy/intl/dpc-v-facebook/cjeu/.

Maximillian Schrems v. Data Protection Commissioner. Disponível em: < https://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=en>.

RULE, James B. Privacy in peril: how we are sacrificing a fundamental right in Exchange for security and convenience. Oxford: Oxford University Press, 2007. P. 135-139.

PANETTA, Rocco. Il Trasferimento All'estero dei Dati Personali, Persona e Mercato Dei Dati. Riflessioni sul GDPR, a cura di GALGANO, Nacia Zorzi. Wolters Kluwer CEDAM, 2019. P. 364-365.

FANNESSY, Caitlin. The Privacy Shield review and its potential to impact Schrems II.05 de novembro de 2019.Disponível em: <https://iapp.org/news/a/the-privacy-shield-review-and-its-potential-to-impact-schrems-ii/.

Principais hipóteses de transferência internacional de Dados Pessoais. Agosto de 2020. Disponível em: https://opiceblum.com.br/infografico-principais-hipoteses-de-transferencia-internacional-de-dados-pessoais/.

VIEIRA, Victor Rodrigues Nascimento. Lei Geral de Proteção de Dados: Transferência Internacional de Dados Pessoais. Disponível em: https://vieiravictor.jusbrasil.com.br/artigos/726523659/lei-geral-de-protecao-de-dados-transferencia-internacional-de-dados-pessoais.

SOLENNE, Vincenzo. Il trasferimento dei dati personali dopo la sentenza Schrems II. Disponível em: https://www.pandslegal.it/compliance/trasferimento-dati-personali-dopo-schrems2/.

ROCHA, Inês. Max Schrems. "Herói da privacidade" elogia cancelamento de envio de dados dos Censos para os EUA. Disponível em: https://rr.sapo.pt/especial/mundo/2021/07/12/max-schrems-heroi-da-privacidade-elogia-cancelamento-de-envio-de-dados-dos-censos-para-os-eua/245548/.

SCHREMS, Max. Statement on EU Commission adequacy decision on US. Disponível em: https://noyb.eu/en/statement-eu-comission-adequacy-decision-us.

SCHREMS, Max. New US Executive Order Unlikely to satisfy EU Law. Disponível em: https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

ZAWADZIŃSKI, Maciej. Un nuovo data transfer deal tra UE e USA, ma niente sarà più come prima di Schrems II. Disponível em: https://www.cybersecurity360.it/legal/privacy-dati-personali/un-nuovo-data-transfer-deal-tra-ue-e-usa-ma-niente-sara-piu-come-prima-di-schrems-ii/.