Consequences of Schrems II case: could the specific consent of art. 49 (1) of the GDPR be used as a regular legal basis for cross-border data transfers?

Amanda Costa Novaes[1]

Abstract: In this article, it is analyzed to what extent there is, after the Schrems II decision, the possibility of using the consent of art. 49(1) of the General Data Protection Regulation (GDPR) as a regular mechanism for international data transfer. Thus, the current understanding and requirements of the European legal system are examined for such scenario. Also, consent as a tool to limit fundamental rights is considered in order to determine if it should be used for cross-border data transfer. Hence, the assessment methodology will be focused on the European Legislation, selected relevant Court decisions and theoretical literature.

1. Introduction

The transfer of data between countries are a common phenomenon in the business model of an internet-based globalized world. Even though it is widely spread, some data flows are especially important due to the economic and politic forces of its agents, such as the ones between countries of the European Union and the United States of America. In this scenario, tensions arose from the American politics of national

[1] Master's student of Business Law and Technology at NOVA School of law, researcher at Whatnext.law.

security and the European fundamental right of data protection, culminating, on July of 2020, in the preliminary ruling by the Court of Justice of the European Union (CJEU) of a case known as Schrems II.[2]

After putting in check the most common legal basis for data exportation of the General Data Protection Regulation (GDPR) [3] between Europe and United States of America (USA), this decision left business without a secure legal ground to make this international transfer, especially online platforms from the United States, which tend to make this in on a daily basis. Although a new agreement for an adequacy decision between USA and the European Union is being currently developed, known as the new data privacy framework, many fear that the core incompatibilities of both political entities cannot be conciliated.

No wonder, in 2021, in a pool lead by the International Association of Privacy Professionals (IAPP-EY), 59% of privacy professionals said complying with cross-border data flows is their most difficult task.[4] The solution adopted by 25% of them was the use of consent as a data transfer mechanism.[5] However, the use of consent for cross-border data transfer is listed in art. 49 of GDPR as a "derogation for specific situations". Still, could such consent be used as a regular tool for data transfer to third countries, after the Court's Decision on the Schrems II Case?

Hence, the general objective of this paper is to conclude if, after the CJEU decision in the Schrems II case, the consent of art. 49(1)(a) of the GDPR can be used as a regular legal basis for international data transfers. The specific objectives are: (a) exam if the requirements of the law and jurisprudence for this specific consent allow it to be used as a regular mechanism; and (b) analyze the theory of consent as tool

[2] CJEU Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems 16 July 2020 EU:C:2020:559.

[3] 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) (2016) OJ L119/1.

[4] IAPP-EY, "Annual Privacy Governance Report 2021" (2021) 21 Available at https://iapp.org/resources/article/privacy-governance-report/ accessed 3 February 2023.

[5] Ibid 23.

to limit fundamental rights, in order to assess whether the same understanding should be adopted on the right of data protection in cross-border data flows.

For this, exploratory research was conducted. Moreover, the assessment methodology focused on: (a) the European legislation granting the fundamental right to data protection; (b) selected relevant Court decisions interpreting fundamental rights and its limitations; and (c) theoretical literature in the matter. In Section 2, the Schrems II Decision and its consequences will be briefly analyzed. Afterwards, in Section 3, there will be detailed the requirements of a valid consent in the General Data Protection Regulation, both the general consent for data processing (art.6) and the specific for international data transfer (art.49). Subsequently, in Section 4, a more theoretical approach of consent to limit fundamental rights will be adopted. In the end, it will be concluded to what extent consent could – or should – be used as a data transfer mechanism.

2. Consequences of the Schrems II Case (C-311/18 CJEU)

Until 16 of July 2020, the data transfers between United States of America and Europe mostly relied on art. 45 of the GDPR, specifically on the Privacy Shield agreement, which stated that the United States had the same level of data protection as the European Union. Yet, on the Schrems II decision, the CJEU declared that this agreement was invalid. This was, in summary, due to three main aspects: (a) the possibility of American Security Agencies, with non-judiciable activities, process bulk collections of personal data trough companies like Facebook; (b) the impossibility of EU citizens accessing effective legal remedies to ensure their data protection rights; and (c) the general primacy of national security over data protection that exists in the United States.[6]

[6] Data Protection Commissioner (n 1), paras 192-201.

With this decision, the most used legal basis for data transfer between EU and USA, grounded on art. 45 of the GDPR, was invalidated with *ex-tunc* effects. Consequently, companies were left in high risk of liability for past transfers based on this decision.[7] The risk is even higher, since the negotiations between States demonstrate a core incompatibility between the national security policies of the United States and the fundamental data protection right in Europe, so new adequacy decisions, as the new data privacy framework currently being developed, can also be invalidated in the future. Consequently, at any time huge costs can be created for companies due to unlawful transfers based on such invalid agreements.

Regarding art. 46 of the GDPR, namely the use of Standard Contractual Clauses to export data to the USA, the Court decided that they need complementary measures to guarantee protection.[8] However, two considerations can be made in this regard. First, those are contractual mechanisms that cannot be ensured in face of the government if it demands data for national security reasons. The second is that the decision did not make clear which mechanisms would actually ensure the data security. Hence, companies are – as well – in risk of implementing contractual or even technical measures for transfer data internationally and, in the future, those being considered not enough to compensate for the lack of protection in the third country.[9]

The CJEU concluded that this did not create a legal vacuum, since art. 49 of the GDPR "details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under art. 45(3) of the GDPR or appropriate safeguards

[7] TRACOL, Xavier, "Schrems II: The return of the Privacy Shield" (2020) 39 Computer law & security review, 8. Available at www.sciencedirect.com/science/article/pii/S0267364920300893 accessed 3 February 2023.

[8] Data Protection Commissioner (n 1), para 133.

[9] MELTZER, Joshua P. "After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals" (2021) 2(1) Global Privacy Law Review, 87. Available at https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021007 accessed 3 February 2023.

under art. 46 of the GDPR".[10] In this scenario, art. 49(1)(a) of the GDPR allows cross-border transfers if the data subject has explicitly consented to it, after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards.

Even though the CJEU decision on the Schrems II case highlighted that art. 49 of the GDPR could still be applied, it also states that this data transfer mechanism is a "derogation for specific situation", which leads to an interpretation of, in essence, it being exceptional. Then, companies were left with no secure legal basis to transfer data to the United States, creating a high risk of responding for material or even non-material damages suffered by the data subject, as stated in art. 82(1) of the GDPR. They were also put in danger of having to pay the fines specified in art. 83(5)(c) of the GDPR, which can go up to 20 million euros or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year.

The tension culminated until the point where the Irish Data Protection Commission, in September 2020, demanded Facebook/Meta to stop exporting data to United States, and, in response, the company affirmed that if that was the case, it would stop its activities in Europe.[11] Now, the EDPB adopted a dispute resolution decision concerning a draft decision of the Irish Data Protection Authority on the matter.[12] In this scenario, since art. 49 of the GDPR was mentioned in the Court's Decision as the basis for inexistence of a legal vacuum to make international transfers, also considering the personal autonomy and freedom to contract of European citizens, should data subjects be able to consent

[10] Data Protection Commissioner (n 1), para 202.

[11] BEESLEY, Arthur, "Facebook's Meta facing order from Irish regulator to suspend data transfers to US" *The Irish Times* (Dublin, 22 February 2022). Available at www.irishtimes.com/business/facebook-s-meta-facing-order-from-irish-regulator-to-suspend-data-transfers-to--us-1.4808534 accessed 3 February 2023.

[12] 'EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT' (13 April 2023) <https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and--creates-task-force-chat-gpt_en?mkt_tok=MTM4LUVaTS0wNDIAAAGLGpYNZFqROYpy4BUfa0wqSL4bSi6aLZ_2QXGb6JnYRcOjc8Cu6TuUKfDuBu0cmXYyqdGoKT2UPKJ5AMS5RXAQYB4lh0RMq54ddmE3l9mQK-wD> accessed 15 April 2023

with this data exportation in order to be able to use, for example, Facebook/Meta online services?

3. Consent in the GDPR and the special requirements of art. 49(1)(a)

Consent is accepted in art. 6(1) of the GDPR as a general legal basis for data processing. Nonetheless, the specific consent to perform cross-border data transfers shall be different from the one for data processing in general, according to the European Data Protection Board (EDPB) Guidelines 2/2018.[13] In this sense, both consents have specific requirements that need to be met. Concerning the consent of art. 49 of the GDPR, for international data transfers, it needs to comply with all the requirements for the two forms of consent, both the general and specific ones.

3.1. Validity of consent for data processing (art. 6(1) of the GDPR)

Consent is accepted as a mechanism to proceed with a lawful data processing, consonant art. 6(1) of the GDPR. In order to be valid, before accepting its terms, the data subject must have informational self-determination, meaning that he or she shall know all the risks and important factors involved with such data processing. This is an effort to prevent abusive privacy policies, as specified in several guidelines of the Data Protection Authorities.[14]

Hence, in order to be valid, in summary, consent shall be: (a) voluntarily given; (b) specific to each processing; and (c) with information about the controller's identity, what kind of data will be processed, how

[13] European Data Protection Board (EDPB), "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679", 7. Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en accessed 3 February 2023.

[14] See GDPR consent guidance of the Data protection authority UK and Guidelines on Consent by the Data Protection Working Party.

it will be used, and the purpose of the processing operations. The possibility of withdrawing consent must always be given and informed to the data subject. Lastly, consent must be unambiguous, granted by a clear affirmative act, which, according to the interpretation of the Court of Justice of the European Union, means an opt-in design.[15]

The main idea here is that a consent request actually makes the subject pause and reflect about the consequences of such act. As it is affirmed by Schermer, Custers and Van Der Hof, "In a sense, a consent transaction functions as a warning that a potentially harmful or legally meaningful moral transformation will take place that requires the (undivided) attention of the individual".[16]

In this way, in order to maintain the possibility of refusing or withdrawing consent, there should be an alternative to perform the service without it. This is because, denying or withdrawing consent and, consequently, being prevented from having access to the service, might have such a big negative impact in the life of the data subject that give him no other option other than to consent with it.[17] Consequently, in the case of international data transfers, the necessity of consenting with such transfer in order to be able to use the service would remove the 'freedom to consent' of the subject.

Hence, there should be a second possibility of performance of the service, either without the cross-border data transfer or through other transfer mechanism. This is due to the fact that, to comply with the freedom to consent and possibility of withdrawing, the data subject must have access to the service even if he or she declines to consent. The EDBP Guidelines highlights that the necessity of maintaining the

---

[15] See CJEU Case C-673/17 Bundesverband e.V. v Planet49 GmbH 01 October 2019 EU:C:2019:801.

[16] SCHERMER, Bart W., CUSTERS, Bart and VAN DER HOF, Simone, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection" (2014) 16 Ethics Inf Technol 171, 172.

[17] VAN CASTEREN, D.C.J., *Consent now and then*, Tilburg University, 2017, 14. Available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://arno.uvt.nl/show.cgi?fid=143636 accessed 02 February 2023.

possibility of withdrawing consent at any time might make it not a "feasible long-term solution for transfers to third countries".[18]

Then, although consent, in theory, could be used as an international data transfer mechanism, in order to be valid, it needs to comply with the necessary aspects to ensure a self-determination of the data subject. In this sense, there would be the necessity of creating a process where consent is not the only possible form of providing the service, in order maintain the data subject's freedom, while also being unambiguous. Nonetheless, if done so, all the requirements for a valid consent, as current interpreted, could be met.

3.2. Requirements of art. 49 of the GDPR

In addition to the requirements for the validity of consent in general, there are also the specific requirements of art. 49 of the GDPR, which claims to be a mere "derogation for specific situations". Hence, also in line with the Schrems II decision, this is a subsidiary possibility. To invoke it, first of all, the controller must reasonably explain why it was not possible to rely on the appropriate safeguards of art. 46 and 47 of the GDPR, as outlined by the European Data Protection Board. [19] After that, it shall be proven that the consent was valid, meaning that the data subject have the necessary information to give permission to the limitation of its fundamental right of data protection.

Thus, according to this article, there is also the necessity of informing all categories of data recipients and countries where data will be transferred. In addition, the data subject must be communicated of the possible risks of the exportation, due to the lack of an adequacy

[18] European Data Protection Board (n 13), 8.

[19] European Data Protection board, "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems", 4. Available at https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en accessed in 03 April 2023.

decision and appropriate safeguards.[20] According to the EDPB Guidelines, this notice can be standardized, but it "should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country."[21] In this sense, the idea is to comply with the informational self-determination and give the subject all the information concerning that transfer in a clear way.

One issue raised here is that those are, in many times, complex information that simply cannot be passed in a clear and simple way to non-experts in the field. Then, it is considered that both the overload of information and transactions, as well as the absence of meaningful choice, negatively impacts the efficiency of consent in a practical way.[22] According to Schermer, Custers, and Van der Hof: [23]

> "As data processing becomes more and more complex, more factors need to be taken into account. The result is that the reality of data processing will become even further removed from the simplistic mental models employed by data subjects. This undermines the basic notion of consent, as it may be argued that consent is not fully informed and truly transformative, when the person who consents is unable to comprehend the consequences".

However, although difficult, and debatable the attention given to consent forms due to the overload of them, it is not impossible to find a design that put such information in a way that is considered specific enough while being clear to the data subject as well. Also, considering that the subject would have an actual choice on whether to consent or not, with the possibility of refusal and still using the service, as above

[20] European Data Protection Board (n 13), 8.
[21] European Data Protection Board (n 13), 8.
[22] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 10.
[23] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 11.

mentioned, there would not be an absence of choice to negatively impact efficiency of consent in this scenario.

Other requirements present on art. 49 of the GDPR are the non--repetitiveness and limited number of data subjects, which are the ones that translate more with the idea of it being a "derogation for specific situations". However, transfers made on basis of specific consent do not have to comply with those characteristics, as highlighted in the recital 111 of the GDPR and in the EDBP Guidelines. *In verbis*, "Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to 'occasional' transfers, while such limitation is absent from the 'explicit consent derogation'".[24] Then, in this point, the regular use of such data transfer mechanism, *per si*, would not be an infringement of the law, since it can be repetitive and without limitation of number of data subjects.

Nonetheless, the premise of art. 49 of the GDPR is only being exceptional, since is supposed to be a "derogation for specific situations", which leads to a restrictive interpretation. In this subject, also according to the EDBP Guidelines, "These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions".[25] Yet, as above mentioned, in the Schrems II decision, the court asses that exactly this article would mean an absence of legal vacuum if it is not possible to use neither the legal ground of art. 45 and 46 of the GDPR to make international data transfers. [26]

Corroborating with the possibility of further use of this legal basis for cross-border data transfer, Professor Dr. von Danwitz, judge--rapporteur in both Schrems cases, on the German celebration of the 40th Data Protection Day, gave a personal statement about the possibility on expanding reliance on Article 49 GDPR derogations in the absence of an adequacy finding. In his words, "the opportunities granted by Article 49 have not been fully explored yet. I believe they are not so

[24] European Data Protection (n 13), 5.
[25] European Data Protection (n 13), 4.
[26] Data Protection Commissioner (n 1), para 202.

narrow that they restrict any kind of transfer, especially when we're talking about transfers within one corporation or group of companies".[27]

In this sense, given that the provision of art. 49 of the GDPR is brought up almost as a solution to a possible legal vacuum created on the impossibility of using art. 45 and 46 of the GDPR, and considering that the provision of the law does not prohibit the repetitive use and for an unlimited number of data subjects, as a logical consequence, the consent of art. 49(1)(a) can and shall be used in such a case. Also, the situation of having a state with a core incompatibility, inhibiting an adequacy decision or insurance of appropriate safeguards, such as United states' politics of national security, could be interpreted as a specific situation that allows the derogation proposed on art. 49 of the GDPR.

The ponderation commonly made here is that, ultimately, this would be "contrary to the previously-stated policy objective and could even ultimately be less protective for data subjects".[28] Although this is a true statement, given the above mentioned interpretation, the use of consent as a regular mechanism for cross-border transfer is not prohibited by law. Also, considering the necessary characteristics to the consent form, a fine level of protection can be achieved. In that regard, if there is a consent that is freely given, actually giving the data subject a choice in order to decline consent and still so use the service, also with the appropriate information about the risks of the transfer in a clear way, the data subject can be empowered with self-determination to make a clear and valid choice.

On the other hand, if the interpretation of data protection rules is so restrictive that impossibilities the use of consent as a ground for international transfer, it can remove from the data subject the alternative of making such conscient choice. Consequently, the citizen could be left

[27] DANWITZ, von, "Europäischer Datenschutztag 2021" (2 February 2021). Available at https://www.youtube.com/watch?v=2hyETsfhErg&t=4320s Accessed 2 February 2023.

[28] RONCO Emmanuel, GERLACH Natascha and FARMER Natalie, "Recommendations of the EDPB Further to the CJEU's Schrems II Judgment: One Step Forward, Two Steps Back?" 2(1) Global Privacy Law Review, 95. Available at https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021008 accessed 03 February 2023.

without the possibility of contracting the service at all, as in the Facebook/Meta example, which translate in such an intervention of the state that inhibits the individual's autonomy to contract.

4. Consent as a tool to limit fundamental rights

No fundamental right is absolute, the possibility of limitation is established in art. 52 of the Charter of Fundamental Rights of the European Union (EU Charter). In that light, the personal autonomy can balance the individual's fundamental right, since it is possible to consent to a limitation of it. This is acceptable, for example, when deciding to make a procedure that harms the person's physical integrity, such as body piercing, or even to refuse medical assistance, threatening the subject's right of life, as decided in the case Jehovah's Witnesses of Moscow and Others v. Russia.[29] In this sense, it is a established idea, according to the jurisprudence of the European Court of Human Rights (ECtHR), that the state cannot "protect the individual against himself".[30]

One consequent fundamental right from the personal autonomy is the freedom to contract, which, even though is not explicit in primary Community law, according to the doctrine, "it is nonetheless comprehensively safeguarded through other guarantees found therein"[31] and "enjoys comprehensive recognition in the jurisprudence of the Court of Justice".[32] Therefore, in the analyzed scenario, consent would be used as a tool to consider that the individual freedom to contract can override the subject's right of data protection, if chosen to, even in a case of transfer to a third country without the same level of protection of the European Union.

---

[29] European Court of Human Rights (ECtHR) Jehovah's Witnesses of Moscow and Others v. Russia App no 302/02 (10 June 2010).

[30] VAN DROOGHENBROECK, Sébastien, *When Human Rights Clash at the European Court of Human Rights: Conflict or Harmony?* (OUP 2017), 67.

[31] BASEDOW, Jürgen, "Freedom of Contract in the European Union" (2008)6 European Review of Private Law 901, 909.

[32] Ibid 913.

Along these lines, recital 4 of the GDPR highlights that data protection "is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality", enabling the analysis in face of freedom to contract. After all, the impossibility of such free will would ultimately mean an absolute data protection right and lead to a state that protect the individual against himself, which is unacceptable.[33]

If briefly analyzed this possibility under the guidelines of the EDPS on assessing the proportionality of measures that limit the data protection right, [34] it is possible to conclude that, for instance, the freedom to contract, as an expression of self-determination trough consent to data exportation, can override the fundamental right of data privacy. The assessment must be based on art. 52 of the EU Charter, which defines that any limitation of fundamental rights must be: (a) provided by the law; (b) respect the essence of the right; (c) meet objectives of general interest recognized by the Union; and (d) also be necessary and proportionate.

Regarding the first three elements, the limitation is provided by law, given that consent is established in the EU Charter of fundamental rights and in the General Data Protection Regulation as a tool to limit the subjects right to privacy and data protection. It also respects its essence by giving the subject informational self-determination, thus not emptying the basic content of the right. In this sense, the possibility of consenting with data processing empowers the individual to make an informed decision about one's personal data while using the service provided by the company.

Thirdly, the measure meets an objective of general interest, namely the function of data in society, as declared in the recital 4 of the GDPR,

[33] VAN DROOGHENBROECK (n 30).

[34] European Data Protection Supervisor (EDPS) Assessing the necessity of measures that limit the fundamental right to the protection of personal data, 6-7. Available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality--measures_en accessed 3 February 2023.

also in relation to what it can make data subjects achieve and their freedom to contract. So, as stated in the law, data can 'serve mankind', not the contrary. In a way, such interpretation is necessary in order to not trying to protect the subject's data up to the point where he/she is not able to enjoin services that are served for his/her self-interest.

In relation to the necessity test, it should be analyzed the effectiveness of the measure for the objective, alongside with whether it is less intrusive compared to other options for achieving the same goal.[35] In this sense, the consent to have data sent to a third country without the same level of data protection – USA in the *Facebook/Meta* case – is effective to guarantee EU Citizens their freedom to contract online platform's services.

Also, it gives the data subject informational self-determination to decide whether to access the online service and have its data shared internationally, or not. Thus, it can be considered less intrusive compared to other options that share it solely relying on measures that don't give proper information and may not ensure the level of protection, since the government can override it. Or even share it laying on adequacy decisions that can, at any time, already be invalid, due to the *ex-tunc* effects of invalidation.

Additionally, the measure is proportionate, since the disadvantages of risking the subject's data protection with the transfer are outweighed by the advantages of respecting the individual's autonomy to contract and ensuring informational self-determination. Highlighting that the measure is the possibility of consent by the data subject, to ensure his/her freedom, not necessarily the transfer itself. Ultimately, the individual should have the power to decide if it wants to protect or limit his/her data protection fundamental right.

To that end, scholars alert to the overload of consent and the impossibility of it being well-informed, leading to the data subject waiving

[35] Ibid 5.

its rights without really comprehending it.[36] Therefore, a case-by-case analysis should focus on the specific consent that was given, making sure it was not abusive, given all the previously mentioned requirements. Also, the controller must have reasons on why it was not possible to ensure one of the appropriate safeguards of article 46 and 47. This residual characteristic of consent to perform cross-border transfers follows both from the rationale of the articles of the GDPR and the CJEU decision in the Schrems II case, as mentioned above. [37]

In that sense, the challenge would be to prove the impossibility of ensuring one of the previous legal grounds and, most of all, have a well--informed and freely given consent. Nonetheless, if it was the case and the consent was, in fact, valid, the person should be able to contract the service accepting the data transfer. After all, if the information is put in a clear way and subjects choose not to give it proper attention, it still falls in their personal autonomy.[38] In addition, there are technical measures that can better inform the subject and facilitate its act of consenting.[39]

Even so, in one hand, the absence of the possibility to consent with the data transfer in order to use the service can be an intervention of the state in the individual's life that is too severe, given that the possibility of consent with a limitation of one's fundamental right apply even for the right of life. However, on the other hand, allowing the data protection of the subject limits itself to a single clause which will probably be ignored by the person in order to use the service, does not balance the power imbalance of huge entrepreneurs that profit billions from the subject's data and the individual himself, as the GDPR aims to do.

Nonetheless, both objectives can be met by a consent that is actually valid, namely given by a person with self-determination to do so, informed and conscient about the risks of the transaction, also with a

[36] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 177-178.

[37] Ibid 24.

[38] BETKIER, Marcin, *Privacy Online, Law and the Effective Regulation of Online Services* (CUP 2019), 30.

[39] Ibid ch 6.

parameter of what will be done with his/her data. In this case, both the empowerment of the individual aimed by the GDPR, and the protection of one's freedom to contract, can be met in order to allow a better data management without such a protection of data that impedes the individual's free will. After all, since consent is a tool to limit fundamental rights stated both in the EU Charter and in the GDPR, it should be ensured to allow cross-border data transfers.

5. Conclusions

In the Schrems II decision, the Court of Justice of European Union invalidated the most common grounds for international data transfer to the United States of America, leaving companies with high risk of being hold liable, due to the difficulty of complying with art. 45 and 46 of the GDPR. In that scenario, art. 49(1)(a) of the GDPR states the possibility of transfers based on specific consent of the data subject. Even though this provision is described as a "derogation for specific situation" and commonly had a strict interpretation, the CJEU Decision on the Schrems II Case highlighted that the absence of possible compliance with art. 45 and 46 of the GDPR would noy create a legal vacuum, due to the provisions of art. 49 of the GDPR.

Therefore, using the specific consent of art. 49(a) of the GDPR as a regular legal basis to transfer data to third countries without the same level of protection of the European Union is compatible with the provisions of the law, as long as fulfilled the requirements for a valid consent. This is mostly because, even though described as a "derogation for specific situation", it does not have to be non-repetitive or to a limited number of data subjects, as have other derogations. Nonetheless, it shall be a different consent than the one given for data processing in general, also informing categories of data recipients and countries where data will be transferred and the possible risks of the exportation, due to the lack of an adequacy decision and appropriate safeguards.

Beyond those specific requirements, in order to be valid the consent shall also respect: (a) the freedom to consent, which would imply in the necessity of an alternative to the consent being withdraw or declined and the service still be provided; and (b) give clear and accurate information, in order to properly give the data subject, the possibility of making a conscience choice about the usage of his or her data. Although it can be tricky to meet all those requirements, there is no factual contradiction that makes it impossible to achieve.

However, despite not being expressively prohibited by any provision of the law, more use of consent forms can generate an overload of consent and be contrary to the policy objective, practically forcing the data subject not to give the proper attention to the information due to its amount. Moreover, the interpretation currently given by the EDBP guidelines to the law do not consider possible to use consent as a regular mechanism for cross-border data transfers, asserting that the consent of art. 49 of the GDPR is an exceptional hypothesis.

Nonetheless, such strict interpretation, inhibiting the use of this mechanism as a regular legal basis for international data transfer, would contradict the Court's decision that point out its usage as an absence of legal vacuum. Moreover, it would not allow the subject to consent with the limitation of his/her fundamental right in order to contract the service, implying in a state that "protect the individual from himself", which is not accepted in the European jurisprudence, not even for the right of life.

Hence, the main point in an assessment of the validity of using consent as a legal basis to make international data transfer should be to verify if the consent in case is not abusive, so it may serve properly as a tool to allow informational self-determination. After all, the GDPR ensures in its recital 4 that "the processing of personal data should be designed to serve mankind", not the contrary. As so, although named as a "derogation for specific situation", given it is not prohibited by law, it should be possible to use the specific consent of art. 49(1)(a) of the GDPR as a regular legal basis to transfer data to third countries

without the same level of protection of the EU, as a consequence of the personal autonomy and freedom to contract.