BRATISLAVA LAW REVIEW

PUBLISHED BY
THE FACULTY OF LAW,
COMENIUS UNIVERSITY
IN BRATISLAVA

ISSN (print): 2585-7088
ISSN (electronic): 2644-6359

SCHREMS II: WILL IT REALLY INCREASE THE LEVEL OF PRIVACY PROTECTION AGAINST MASS SURVEILLANCE? / Lusine Vardanyan, Václav Stehlík

Lusine Vardanyan
Ph.D. researcher at Palacky University in Olomouc, Law Faculty, Department of International and European Law, 17. listopadu 8, 779 00 Olomouc, Czech Republic;
lucyrossetti77@gmail.com
ORCID: 0000-0002-2981-0520

doc. JUDr. Václav Stehlík, LL.M. Ph.D.
Associate Professor of EU law, at Palacky University in Olomouc, Law Faculty, Department of International and European Law, 17. listopadu 8, 779 00 Olomouc, Czech Republic;
vaclav.stehlik@upol.cz
ORCID: 0000-0003-1997-7965

The paper was prepared under project no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation (GAČR)

Abstract: *An important event that once again brought to the forefront issues related to mass surveillance was the judgment of the Court of Justice of the European Union (hereafter referred as CJEU) delivered on July 16, 2020 in the case of Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems (Schrems II). It can be considered as the first serious precedent in the field of surveillance, which is aimed at ensuring privacy in the field of national security. Therefore, it becomes an important issue to assess its impact on the legal framework of international transfers of personal data and on the level of privacy protection. The impact of the judgment on the level of privacy protection and mass surveillance is particularly important now that COVID-19 contact tracing programs are being widely used. In this research we try to trace the formation of the approach to mass surveillance in the case-law of CJEU before and after the Schrems II. We also try to point out some of the difficulties that the process of cross-border data transfer will face after the Schrems II. The main question of the study is whether the approach of the CJEU developed in the Schrems II will actually increase the privacy protection against mass surveillance. We conclude that the Schrems II is an important decision with serious consequences that go beyond the direct impact on data transfer between the EU and the US. It can have controversial influence of the level of privacy protection. Together with the positive trend of formation of more harmonized global data protection standards it can create many unresolved problems in the field of international data transfer and in economic dimension.*

Key words: *Court of Justice, privacy, mass surveillance, Schrems I, Schrems II., EU Law*

Suggested citation:
Vardanyan, L., Stehlík, V. (2020). Schrems II: will it really increase the level of privacy protection against mass surveillance? *Bratislava Law Review*, 4(2), 111-128.
https://doi.org/10.46282/blr.2020.4.2.215

Submitted : 18 November 2020
Accepted : 04 December 2020
Published : 31 December 2020

1. INTRODUCTION

The issues of "mass surveillance" have again become relevant in connection with the COVID-19 and the choice of contact tracking apps to combat it, which also give an opportunity to collect and store personal data.

On March 23, 2020, the European Commission met with Telecom operators to discuss the issue of data collection and processing. This is a consequence of the fact

that on March 19, 2020, the European Data Protection Supervisor (further referred as EDPS) suspended a ban on the processing and exchange of personal information of European citizens. In his statement EDPS confirmed, with reference to the General Data Protection Regulation (hereinafter - GDPR), that this is now allowed for "*competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein*" (European Data Protection Board, 2020). Relying on this legal relief, the Internal Market Commissioner Thierry Breton contacted eight phone operators[1] and received the approval of all companies, thus, paving the way for an unprecedented project at the European level. The Commission will collect, combine and analyse personal data to ensure European coordination in the fight against Covid-19 and only the Commission will be responsible for any possible violation. As Breton said "*Digital technologies, mobile applications and mobility data have enormous potential to help understand how the virus spreads and to respond effectively*" (European Commission, 2020c). The Thierry Breton's Office wants to simulate the spread of the epidemic in the territory in real time and check the "*(...) link between containment measures and the spread of the virus*" (Untersinger, 2020) to assess the effectiveness of this containment. The European Data Protection Supervisor Wojciech Wiewiórowski in an open letter to Roberto Viola, the Director-General of DG CNECT, states that *"...the data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics*" (2020).

Another important event that updated the problems associated with mass surveillance was the decision of the Court of Justice of the European Union (hereafter referred as CJEU) on July 16, 2020 in the case of Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems.[2] At first glance, this ruling is considered to be continuation of the case Maximilian Schrems v. Data Protection Commissioner,[3] which invalidated the Safe Harbor (Decision 2000/520).[4] But despite the fact that in both cases the problem was to ensure the proper level of confidentiality when transferring personal data to EU countries, it is worth noting that the decision on Schrems II was made in a different political situation, in particular Brexit. Moreover, it was made against the background of the existence of extensive national surveillance laws and the legitimization of mass surveillance in the case law of the ECtHR. It seems that the CJEU itself takes into account the above factors when making a decision on the Schrems II.

Schrems II can be considered the first serious precedent in the field of surveillance, which is aimed at ensuring confidentiality in the field of national security. Therefore, it becomes an important issue to assess its impact on the legal framework of international transfers of personal data.

In this research, we will try to trace the formation of the approach to mass surveillance in the practice of CJEU before and after the Schrems II. We will also try to identify the factors that influenced the formation of the approach expressed in Schrems II, and show some of the difficulties that the process of cross-border data transfer will face after Schrems II. This will give us an opportunity to answer the question whether the

[1] Orange, Telecom Italia, Telefonica, Deutsche Telekom, Telia, Vodafone, Telenor and A1 Telekom Austria.
[2] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559.
[3] Schrems I: CJEU, Judgment of the Court (Grand Chamber) of 06 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650.
[4] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), Official Journal L 215 , 25/08/2000, p. 0007 – 0047 (hereafter referred as Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC).

CJEU's approach developed in Schrems II really increases the level of the privacy protection against mass surveillance.

2. THE CASE LAW OF THE CJEU: BEFORE THE SCHREMS II

The development of the approach to mass surveillance in the EU begins with Decision 2000/520/EC, adopted on the basis of DPD.[5] Article 25 (1) of the DPD established the principle that the transfer of personal data to a third country is only possible if the relevant third country provides an adequate level of protection for such data, which may be established by a decision of the Commission. Article 57 of the DPD provided for the possibility of prohibiting the transfer of personal data to a third country when the latter did not provide this level of protection, although article 26 of the DPD knew many exceptions that allowed such transfer to a country that did not provide such protection. To achieve the objective of the DPD to facilitate the free movement of data flows the Commission approved the "Safe Harbor Principles", believing that they would provide "adequate" protection for EU citizens whose data was transferred to the US.[6] Annex I to Decision 2000/520 stated that the obligations imposed by these principles do not apply if justified by "*national security, public interest, and compliance with US law*" and "*legislative, administrative, or judicial decisions, create conflicting obligations, or grant explicit authorizations*", provided that organizations can then demonstrate that non-compliance with the principles is limited to "*measures necessary to safeguard the legitimate interests that the authorization is intended to serve.*"[7] It is clear that Safe Harbor member organizations had a duty to cooperate with intelligence agencies to identify potential violations of national security, and this obligation took priority over respect for the right to protect the personal data. This system was subsequently reviewed by the European Commission in 2002 and 2004. The European Commission issued an official criticism of this Decision.[8]

In October 2015 the CJEU in the case **Schrems I** declared invalid the "Safe Harbor" and concluded that the non-discriminatory nature of surveillance programs conducted by US intelligence services made it impossible to ensure that the personal data of EU citizens is properly protected when shared with US companies. The CJEU noted that "*interference with the right to privacy and the protection of personal data guaranteed by articles 7 and 8 of the EU Charter must … lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards*"[9] and "*derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*".[10] Also the right to effective judicial protection must be respected.[11]

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, pp. 31–50.
[6] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC, pp. 7–47.
[7] Annex I Safe Harbor Privacy Principles issued by the US Department of Commerce on 21 July 2000/, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (accessed on 18.11.2020).
[8] V. Commission Européenne. *Communication au parlement européen et au conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'union et des entreprises établies sur son territoire*, COM(2013) 847 final, 27 novembre 2013.
[9] Schrems I: CJEU, Judgment of the Court (Grand Chamber) of 06 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650, p. 91.
[10] Ibid., p. 92.
[11] See ibid., p. 95.

DOI: 10.46282/blr.2020.4.2.215

CJEU highlighted the extraterritorial effect of the right to protect personal data (see also Scott, 2014) strengthening the CJEU's control over the "*adequate*" level of personal data protection in third countries. While recognizing that the term "*adequate*" implies that such a country cannot be required to provide a level of protection strictly identical to that guaranteed in the EU legal order, the Court nevertheless found that it must be "*substantially equivalent to that guaranteed in the Union.*"[12] The Court also noted that the means used by third country should be read *"in accordance with fundamental rights*", which means that checks are carried out in accordance with the maximum requirements of the Directive.[13] Consequently, the foreign law in question must have an external control mechanism in the form of an independent body, which is a necessary element of any system aimed at ensuring compliance with the rules relating to the protection of personal data. This decision establishes a situation where the Court analyses the foreign law using external standards for it becoming the "new constitutional court" for the right to privacy in third country legislation, but in practice it does not have the authority to enforce its decisions.

The **case of Digital Rights Ireland** is also significant for the topic under consideration,[14] although many EU Member States either did not comply or partially complied with the decision (PRIVACY INTERNATIONAL, 2017, p. 12). In this case the CJEU considered the question of compliance with the EU Charter and Directive 2006/24/EC, which imposed an obligation on providers of electronic communications services to preserve data transmitted through them or generated by them. The CJEU declared this Directive invalid, considering its measures as a disproportionate invasion into the right to privacy and protection of personal data.[15] The main argument was that the goal of fighting organized crime and terrorism does not in itself justify general measures to preserve data; restrictions on the right to privacy and the right to protect personal data should be "strictly necessary".[16]

The CJEU criticized the general scope of the data interception obligation: this measure applied to "*all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*"[17] or for the prevention of "*a threat to public security*".[18] The Court then pointed out that the Directive did not specify any objective material or procedural conditions limiting the access of national authorities to this data and established the need for a monitoring procedure by a court or an independent executive authority.[19] Finally, the period of prescribed data storage was not made dependent on an objective criterion that allowed it to be limited only to what was strictly necessary.[20]

[12] Schrems I: CJEU, Judgment of the Court (Grand Chamber) of 06 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650, p. 73.
[13] Ibid., p. 74.
[14] CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.
[15] Ibid., p. 69, 71.
[16] Ibid., p.51, 52.
[17] Ibid., p. 57.
[18] Ibid., p. 59.
[19] Ibid., p. 60–62.
[20] Ibid., p. 63–64.

The CJEU specified that there is not a ban on states using metadata interception as a preventive measure, but this interception should be targeted[21] and meet a number of requirements. The purpose of data interception should be limited to the fight against "serious crimes"; the principle of strict necessity should be observed when choosing the subject matter, means of communication, data types and time of application of this measure. In particular, national legislation should be based on objective evidence that can convince the public that there is at least an indirect link between intercepted data and the fight against serious crimes.[22]

The conclusions of this case were developed in the case of **Tele2 Sverige AB**,[23] which dealt with requests for the interpretation of article 15 (1) of Directive 2002/58/EC.[24] The principle of strict necessity, according to the Tele2 judgment, should also be observed at the stage of regulating the conditions for national authorities to obtain access to intercepted data: they should only pursue such a goal as the fight against serious crimes.[25] Among the requirements to be met by national legislation the CJEU also indicated prior control by courts or independent executive authorities; intercepted data must be stored within the EU and be permanently destroyed at the end of the storage period; citizens who have been subjected to surveillance must be notified of the operations that have been carried out and a remedy must be available to them.[26] Finally, Member States should ensure that the national legal regime meets the level of protection guaranteed by EU law.

Despite the progressiveness of this decision did not affect the purpose of protecting public safety. Except this, the text of Directive 2002/58/EC itself excludes from its scope of application "*activities concerning public security, defence, state security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*".[27] The CJEU only recognized that Directive 2002/58/EC applied to both the interception and access stages of data, and interpreted its provisions in the light of the Digital Rights Ireland decision. However, this decision, in turn, was also limited to the purpose of fighting crime.

And if in case Tele2 Sverige AB the CJEU believed that only the fight against serious crimes can justify the retention of data, in the case of **Ministerio Fiscal**,[28] it found that limited access to this data can be provided even for the fight against non-serious

[21] CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, p. 108.

[22] CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, p. 57.

[23] CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

[25] CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, p. 103.

[26] See, for example, in the cases: ECtHR, Weber and Salavia against Germany, app. no. 54934/00, 29 June 2006, p. 95; and ECtHR, Zacharov v. Russia, app. no. 47143/06, 04 December 2015, p. 231.

[27] Article 3(2) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[28] CJEU, Judgment of the Court (Grand Chamber) of 2 October 2018, proceedings brought by Ministerio Fiscal. Request for a preliminary ruling from the Audiencia Provincial de Tarragona, Case C-207/16, ECLI:EU:C:2018:788.

crimes. The CJEU clarified that the main threshold is that "*access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails*"[29] and "*when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally*".[30]

So, for the CJEU, the indiscriminate nature of the collection and processing of personal data, even if it is intended to protect the society from serious crimes, violates the content of the fundamental right to respect for privacy and entails significant risks to rights and freedoms and requires that the exceptions to the protection of personal data and their restrictions were applied to the extent strictly necessary. The WP 29, which unites European personal data control authorities, published its first report on the "Privacy Shield", in which it "*recalls its long-standing position that massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights*".[31]

However, despite the fact that the Tele2 ruling deals only with measures taken to fight against crimes, the CJEU's general position on mass surveillance carried out for other purposes can also be drawn from the text of the judgment. Emphasizing that data interception should be restricted to persons suspected of planning or committing a serious crime or otherwise involved in it, the CJEU stated: "*[h]owever, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities*".[32]

The position of the CJEU based on these rulings strengthened the guarantees provided against the abuse of surveillance, and in the discourse of the need to ensure supervision over the excess of laws, since any system of mass surveillance is itself considered a violation of private life. Despite the noted shortcomings the significance of the CJEU's approach in terms of expanding access to courts for citizens, strengthening their procedural guarantees, and condemning the very possibility of mass surveillance should be highly assessed.

After the judgment in case Schrems I Safe Harbor was replaced by the Privacy Shield in accordance with the Decision 2016/1250.[33] But little has changed in terms of surveillance. This enabled Mr. Schrems to continue his campaign. In the new complaint Schrems argued that the US does not provide adequate protection because the US law requires Facebook Inc. to allow access to the transferred personal data of the NSA and the FBI. This means that data is used in a way that is incompatible with the right to privacy, and therefore data transfers via Facebook should be suspended. This became the subject of the Schrems II.

[29] Ibid., p. 55.
[30] Ibid., p. 57.
[31] Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield, Brussels, 13 April 2016. Available at: https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf (accessed on 18.11.2020).
[32] CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, p. 119.
[33] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), C/2016/4176.

3. SCHREMS II: OLD SOLUTIONS AND NEW PROBLEMS

3.1 GDPR: further expansion of the external scope

The desire of expanding the scope of GDPR is not new for the case law of CJEU. In the case Google v CNIL,[34] there were some attempts to address the issue of the territorial scope of the right to be forgotten. The decision was made during the period when the GDPR came into force and the Court did not miss the opportunity to outline the scope of its practical application. At first glance, it can be concluded that the Court held that there is no obligation under Directive 95/46/EC to apply right to be forgotten globally.[35] However, the analysis of the decision allows us to see its other feature: the absence of a fundamental ban on the possibility of recognizing the universal application of the right to be forgotten and the GDPR. Having decided that Google "*must be regarded as carrying out a single act of personal data processing*", the Court subordinates the processing of data by Google on all its domains to the GDPR jurisdiction. The Court rules that GDPR applies to all Google, not just Google France.[36]

The CJEU also allows for further steps to be taken to ensure such universal application, for example by pointing to existence of a competence on the part of the EU law to lay down the obligation to carry out de-referencing globally.[37] In addition, the Court emphasizes that EU law does not prohibit the practice of global de-referencing. It tries to preserve the possibility of such application.[38] And this approach is due to the awareness that a categorical refusal of non-universal application of the right to be forgotten, as well as the GDPR, may make impossible to achieve the EU goal of ensuring a high level of personal data protection. The legalisation of the universal application of the right to be forgotten and the GDPR has set a vector for the case-law of the CJEU in the field of EU data protection, which is also further developed in the Schrems II case.

The Schrems II does not question US surveillance powers as such: personal data of EU data subjects "*transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defense and state security by the authorities of that third country*".[39] Rather, it highlights the lack of effective legal remedies for EU data subjects in the US. And this is how the Schrems II differs from the Schrems I. In the latter case the criticism of surveillance is more pronounced: "*legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by article 7 of the Charter*".[40] Perhaps this is an indirect recognition of the position of the ECtHR, which stated that "*the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation*", adding that such regimes are "*valuable means to achieve the legitimate aims pursued, particularly given the current*

[34] CJEU, Judgment of the Court (Grand Chamber) of 24 September 2019, Google Inc v Commision nationale de l'informatique et des libertés (CNIL), C-507/17, ECLI:EU:C:2019:772.
[35] Ibid., p. 64.
[36] Ibid., p. 37
[37] Ibid., p. 58.
[38] Ibid., p.72.
[39] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 86.
[40] Schrems I: CJEU, Judgment of the Court (Grand Chamber) of 06 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650, p. 94.

threat level from both global terrorism and serious crime".[41] However, this does not mean that the negative attitude towards mass surveillance is easing. On the contrary, the CJEU once again asserts its commitment to the "strict necessity" of conducting surveillance.

The CJEU further states that "*the Authorities of this third country cannot exclude this transfer from the scope of the GDPR in accordance with article 2 (2) of the GDPR*".[42] The justification for this approach is that article 4(2) of GDPR defines "processing" as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means*" and mentions, by way of example, "*disclosure by transmission, dissemination or otherwise making available*", but does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V thereof, entitled "Transfers of personal data to third countries or international organisations", and also confers specific powers on the supervisory authorities for purpose, which are set out in article 58(2)(j) GDPR.[43]

Simultaneously the CJEU argues that article 4 (2) of the TEU, which removes national security competence from the scope of EU law, applies only to the EU Member States.[44] Each EU Member State can balance national security needs with the right to data privacy at its own discretion, but this does not apply to third countries where EU data is transmitted.

In fact, the CJEU ones again turns the GDPR into a legal act of influence to countries outside the EU. European Commission assesses the GDPR "*as a catalyst for many countries around the world to consider introducing modern privacy rules*" (2020a, p. 12). The Court extends the rights and obligations stated by the GDPR to third states that receives personal data from the EU. This aspiration has quite noble goals: through the globalization of its privacy standards, to counter the dangers that arise from the increasing access of international data flows for national security agencies and to increase the level of privacy protection. This approach increases the discrepancy between the application of the GDPR within the EU and beyond, in effect deepening the already existing double standards of privacy protection. This contradicts the EU's clear desire to create global standards for the protection of the privacy.

3.2 The CJEU's repeated insistence on independent courts as the essential guarantors of privacy

In the case Schrems II the CJEU held that Section 702 of the Foreign Intelligence Surveillance Act (FISA) is not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the EU Charter[45] for reasons that this Section "*does not indicate any limitations on the power it confers to implement surveillance programs for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programs*".[46] In addition as a supervisory mechanism "*PPD-*

[41] ECtHR, Big Brother Watch and Others v. United Kingdom, app. no. 58170/13, 62322/14 and 24960/15, 13 September 2018, p. 386.
[42] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 86.
[43] Ibid., p. 82.
[44] Ibid., p. 81.
[45] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 178.
[46] Ibid., p. 180.

28 does not grant data subjects actionable rights before the courts against the US authorities".[47] The Court also rejects Executive Order 12333, which allows access to data transmitted in the US without this access being subject to judicial review.[48] In *Schrems II*, the absence of an independent court assessed as a big disadvantage for US privacy protection. Judicial redress has always been essential to the case law of CJEU in the field of data protection. And in the Privacy Shield, an Ombudsman within the State Department was supposed to serve as the institutional alternative to courts. But the Ombudsman has no guarantees of independence from the US Executive branch[49] or "*the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely*".[50] And the CJEU considers it as an important omission. It concludes that the Commission's decision on the adequate level of protection provided by the Agreement between the EU and the US is untenable.

Note that this is practically the criterion that was mentioned as an important guarantee in in the case Szabó and Vissy v. Hungary.[51] But this is also the criterion that was "abolished" as a result of the easing of the ECtHR's approach to mass surveillance in the case of Big Brothers Watch v. the United Kingdom. Here the ECtHR states that although in the United Kingdom permission to conduct mass surveillance was not issued by either a judge or an independent administrative authority, there are no problems because several indications show that there is no abuse of executive power.[52] Re-emphasizing the importance of the specified guarantee in the Schrems II is another step towards fragmentation of the judicial practice of the two European Courts. Can this be considered an increase in the level of privacy protection? Yes, if we take into account the same legitimization of mass surveillance in the practice of the ECtHR and the need to resist it. We will discuss it below.

3.3 Assessment of compliance of foreign laws by private companies

The CJEU repeated its position from the Schrems I and in determining the level of protection required by the GDPR. It ruled that the level of protection should be "practically equivalent" to the level of protection in the EU. However, the GDPR should be understood in the light of the EU Charter. The Court also stated that the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of GDPR.[53] The CJEU ruled that the use of SCC is required in a third country which "*guarantees the ensuring an adequate level of protection essentially equivalent to that ensured within the Union*".[54] The court interprets articles 46 (1) and (2) (c) in relation to article 45 (2) of the GDPR so that economic operators, when transferring personal data

[47] Ibid., p. 181.
[48] Ibid., p. 183.
[49] See ibid., p. 195.
[50] Ibid., p. 196.
[51] ECtHR, Szabó and Vissy v. Hungary, app. no. 37138/14, 12 January 2016, p. 77, 80, 81.
[52] ECtHR, Big Brother Watch and Others v. United Kingdom, app. no. 58170/13, 62322/14 and 24960/15, 13 September 2018, p. 381.
[53] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 105.
[54] Ibid., p. 104.

on the basis of SCC, must take into account the relevant aspects of the legal system of this third country, including national security, in relation to any access by public authorities of this third country to the transferred personal data.[55] The burden of verifying that a data recipient in the destination country can meet the level of protection required by EU law is borne by economic operators that use SSC and are supervised by the competent data protection authority of an EU Member State.[56]

The content of such legal examination of foreign laws by private companies is unclear. Is it enough just to compare the requirements of foreign laws and GDPR requirements? Is it necessary to compare the GDPR with the practice of national security agencies of third countries? The latter seems difficult, if not impossible. Of course, this position is related to the desire to ensure the priority of fundamental rights over economic development. But this desire is almost impossible to implement in practice. However, companies in this case find themselves in the middle of two fires. On the one hand, when transferring data to a country that laws do not provide the level of protection required by EU law, they may face penalties, on the other hand, if they refuse such transfer, they may be subject to material sanctions within the framework of, for example, contractual relations.

Schrems II, which indicates the invalidity of the EU-US Privacy Agreement, may significantly reduce the flow of personal data from the EU to the US and have a negative impact on the development of international trade and information technology, given that the US is one of the leading powers in the digital economy. Enthusiasm for the GDPR as "*a key reference point at international level*" (European Commission, 2020a, p. 12) may be overshadowed by difficulty data flows after Schrems II. As mentioned in the European strategy for data: "*Today's European companies operate in a connected environment that goes beyond the EU's borders, so that international data flows are indispensable for their competitiveness*" (European Commission, 2020b, p. 23). Therefore, the consequences of the Schrems II can also be reflected in the decline in the competitiveness of European companies. Was this the purpose of the CJEU?

Also note that the Commission itself considers the promoting convergence of data protection standards "as a way to facilitate data flows and thus trade" (2020b, p. 23) and does not consider this promotion as an end in itself. The goal of prioritizing the protection of fundamental rights and creating more harmonized global data protection standards should not be achieved through complete disregard of economic factors; otherwise there may be a rebound effect on the same fundamental rights.

3.4 Schrems II: impetus for the development of constitutional law

One of the reasons for the CJEU's criticism of US legislation was a gap in US constitutional law for non-US persons. The Fourth amendment to the US Constitution provides different levels of legal protection to people in the US compared to those outside the US, including access to US courts. In some European countries, the level of privacy protection in national security surveillance may also depend on the nationality and residence of the data subject. This situation allows for a sharp decrease in the level of protection of privacy, since theoretically it allows surveillance by foreign intelligence agencies of all States whose citizen or resident data subject is not. The condemnation in Schrems II of a similar approach in US law may serve as a signal for many EU Member States to review their similar provisions and a new round in the development of constitutional law. Although according to article 4 (2) of the EU Treaty "*national security*

[55] Ibid., p. 105.
[56] Ibid., p. 135, 137, 142, 146.

remains the exclusive responsibility of each member state", according to the AG Manuel Campos Sánchez-Bordona "*this provision does not exclude that EU data protection rules may have direct consequences for national security*".[57]

Note that the Federal Constitutional Court of Germany is somewhat ahead of the CJEU in this regard. Federal Intelligence Service Act (BND Law BNDG) involves different types of surveillance depending on the nationality of citizens. It allows strategic intelligence by means of communication abroad. The Federal Intelligence Service (BND) does not have the right to such control over the communication of German citizens, as well as within its own borders: such surveillance is a violation of Article 10 of the German Basic Law, which protects the freedom of communications. The legal basis for such activities in relation to foreigners appeared in the security service in 2017 after the amendments to the above-mentioned law. The Federal Constitutional Court of Germany in its decision on 19 May 2020[58] explained that the protection provided by the German Constitution (Basic Law) in relation to German public authorities is not limited to the territory of Germany and protects foreigners in other countries, in this case, in the context of foreign telecommunications surveillance conducted by the BND.

The ruling of the Federal Constitutional Court of Germany is also notable for the fact that it may be a kind of response to some delay in the formation of adequate international standards governing the processing of personal data. National jurisdiction is trying to implement rules with global influence and spread their own privacy standards everywhere. In this aspect the Schrems II are the landmark decision, which mark the beginning of an important stage in creating standards for "extraterritorial" and universal privacy protection by the fact that it will strengthen the role of the GDPR in setting international data protection standards. It undoubtedly will also have an effect the surveillance activities of third countries' intelligence services. It is not yet possible to assess this effect, but we can definitely say that it will increase the level of privacy protection.

3.5 Problematic adequacy decisions after Schrems II

The EU seeks to maintain a high degree of privacy, while at the same time seeking to strengthen its role as a decisive actor in the digital economy. However, the current application of GDPR also introduces some obstacles to achieving these goals. The GDPR is used as a "lash" to force reform of third-country security services. However, this may not have the necessary effect, for example, in the case of those regimes that are not as democratic. Actually if the EU hopes that the approaches of the Schrems II can "force" the US to become more "adequate" due to the damage to its national security due to the economic bonuses from the use of EU personal data, this is in our opinion somewhat naive. After Snowden revelations, US tried to convince the EU that the surveillance of non-US persons was protected although there was no provision for it in US statutory law. The result of this attempt was the Presidential Policy Directive (The White House; Office of the Press Secretary, 2014). But Trump's policies are not so smooth. So perhaps those are

[57] Advocate General's Opinions in case C-623/17 Privacy International, joined cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreauxfrancophones et germanophone and Others, Press release No 4/20, 15 January 2020. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf (accessed on 18.11.2020).

[58] Entscheidung des Bundesverfassungsgerichts - 1 BvR 2835/17 - (zu den §§ 6, 7, 13 bis 15, 19 Absatz 1, § 24 Absatz 1 Satz 1, Absatz 2 Satz 1, Absatz 3 des Gesetzes über den Bundesnachrichtendienst) (BVerfGE20200519 k.a.Abk.), 19.05.2020. AVAILABLE AT: https://www.buzer.de/gesetz/13986/index.htm (accessed on 18.11.2020).

right who after the Schrems II began to doubt that the US will allow to change the US law and to reduce the expense of surveillance.

There is another consequence that may possibly occur - it is challenging already existing adequacy decisions. As it is known, the European Commission also deals with a number of other countries.[59] None of these decisions is secured from judicial challenge after the Schrems II. The problem is that the Commission also makes an adequacy decision on taking into account the economic and commercial component of personal data transfers. This is a broader area for assessing adequacy than the one the CJEU considers and evaluates: ensuring a level of privacy protection consistent with the EU Charter.

As we have already noted, the CJEU in Schrems II subordinates economic interests to basic human rights, which means that if the adequacy assessment was carried out by the Commission based on the priority of the economic factor or taking into account the possible negative consequences of stopping transfers of personal data, then there is a potential possibility of challenge of any of the Commission's decisions on adequacy. Time will tell whether such a scenario will be implemented to review existing decisions.

3.6 GDPR: different consequences for different states

Schrems II does not smooth out the discrepancy between the external (international) and internal (in-European) consequences of applying the GDPR in the field of national security. The CJEU once again makes itself the arbiter of other countries' approaches to data access for national security purposes[60] and formulates requirements for national security agencies of third countries that it cannot impose on its own national security agencies.[61]

Disputes about the limitations of EU legislation in the field of national security become an object of attention of the Court in the rulings, issued on October 6, 2020.[62] The Court tries to answer the question of whether the EU law is applied in the context of the activities of security agencies of Member States. The CJEU found that EU privacy laws, such as the Directive on privacy and electronic communications[63] and the GDPR, cannot be overridden by national security agencies to allow for regular bulk data collection, and the protection mechanisms provided for data processing in the EU Charter are fully applicable in this area as well.

[59] For example: 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Text with EEA relevance); 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539).

[60] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 178.

[61] European Agency for Fundamental Rights 2015. "Surveillance by Intelligence Services: fundamental rights, safeguards and remedies in the EU"; Sidley Austin 2016. "Essentially Equivalent -A comparison of the legal orders for privacy and data protection in the European Union and the United States", January 2016; Opinion of Geoffrey Robertson QC, 14th January 2016.

[62] CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, The Investigatory Powers Tribunal (United Kingdom), in the proceedings Privacy International Case C-623/17, ECLI:EU:C:2020:790; CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.

[63] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

In case La Quadrature du Net the Court states, that all operations processing personal data carried out by providers of electronic communications services fall within the scope of Directive 2002/58, including processing operations resulting from obligations imposed on those providers by the public authorities.[64] **In case Privacy International** the Court states: *"…national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of [Directive 2002/58]"*.[65] Article 4 TEU actually exclude national security from the scope of application of the EU legislation. However, this is narrowly applicable to the activities of intelligence agencies for the protection of national security. Article 4 of the TEU does not cover the activities of service providers where requested or obliged, by national laws adopted in the implementation of Article 23 GDPR and/or Article 15 of Directive 2002/58, to restrict a number of individuals' rights for the purposes of protection of national security.

This is a step in gradually extending the requirements of EU law to the national security sphere of the EU Member States. The position of the CJEU reflected in the rulings of October 6, 2020, makes it possible to clarify the external boundaries of government access to "metadata", leaving them under a high level of protection in the EU, even if it is used for national security purposes. These decisions provide more detailed guidance on the standards that national security laws must meet. And together with Schrems II, they lay the groundwork for the upcoming decisions of the European Commission on the adequacy of a third country in relation to the transfer of personal data from the EU under the GDPR.

Note that in the case **La Quadrature du Net and Others**[66] the Court still allows general and indiscriminate storage of traffic and location data, in the event of a "*serious threat to national security*". The Court provides an opportunity for Member States to reform their laws by circumventing the position expressed in Tele 2. The ambiguity of concepts, describing the presence of threat to national security and identification of activities that pose a threat to national security by the Member State itself may lower the level of protection of the right to privacy. The equalization the external (international) and internal (in-European) consequences of applying the GDPR in this situation may also lower the level of protection in the field of international data flows, established by the Court in Schrems II. Anyway, it is clear that at the time of making a decision on the case Schrems II, the Court has shown a determination to continue fighting unjustifiably broad surveillance laws.

4. SOME FACTORS CONTRIBUTING TO THE FORMATION OF APPROACHES IN SCHREMS II

4.1 Brexit

Despite many provisions in Schrems II are repeating the provisions of Schrems I, Schrems II is not a complete continuation of Schrems I: it appears in a very different legal

[64] CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, p. 94-97, 101.
[65] CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, The Investigatory Powers Tribunal (United Kingdom), in the proceedings Privacy International Case C-623/17, ECLI:EU:C:2020:790, p. 49.
[66] CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, p. 141.

DOI: 10.46282/blr.2020.4.2.215

and political discourse. Moreover, it seems that the Court itself also proceeded from these events. Among such facts: Brexit; the existence of extensive national surveillance laws; the legitimizing mass surveillance in case law of the ECtHR.

An indirect consequence of Schrems II may be a complication of the future EU and UK compliance decision. In the UK, as in the US, there is a mass surveillance system. As an EU Member State, the UK's national security surveillance practices did not fall within the scope of EU law, and the country was free to receive and transmit personal data within the digital single market. After Brexit, when the UK becomes a third country, data transfers will be regulated by Chapter V of the GDPR and the UK legal system, including national security, must provide a level of protection almost equivalent to that guaranteed in the EU. The Court's attitude to mass surveillance in Schrems II case indirectly endorses this approach to the UK. The CJEU makes it clear that after Brexit, all aspects of the UK's privacy regime, including national security, are subject to the adequacy requirement. Whether the existing supervision and an independent court will be sufficient for this is unknown.

Moreover, the CJEU stated that the third-country adequacy analysis is entirely based on the GDPR, whose requirements must be understood in the light of the EU Charter as interpreted by the Court itself[67] not the ECtHR. It may be reminded that the ECtHR sets more lenient criteria for surveillance, but even in this case, the ECtHR has repeatedly condemned UK laws for non-compliance with the ECHR standards.[68] The new UK law on intelligence services is now also being challenged in the ECtHR. If the ECtHR again finds that the new law does not comply with the ECHR standards, the European Commission cannot approve the adequacy of UK laws to EU legislation standards that are stricter than the ECHR standards. The threat of legal challenge in the CJEU is almost guaranteed. In light of this, getting an agreement on adequacy for the UK may be a difficult task for a long time to come.

4.2 Legitimation of mass surveillance in the case law of the ECtHR and opposition to it by the CJEU

After terrorist attacks since 2015, most European countries have adopted new, almost identical laws that allow mass surveillance on broad grounds. Thus, many laws allow extensive opportunities for mass surveillance of foreigners, where the victims of potential abuse are non-citizens with few legal protections for redress. The ECtHR has almost come to terms with this state, which cannot be said about the CJEU.

For the CJEU this issue can have two directions of decision: either the adoption of the position of the ECtHR as a determining weather vane through the use of potential of article 52(3) of the CFR, or deepening the existing fragmentation of case laws. As it is known, the CJEU is trying to minimize the effect of article 52(3) of the EU Charter.[69] The CJEU has shown that the autonomy of the EU's legal order is an absolute priority for it. It seems that the second direction will be preferable for the CJEU and Schrems II showed that the CJEU supported its already expressed position based on its previous case law. Today we have a fragmentation of the case law of the ECtHR and the CJEU. The Schrems II deepens it.

[67] Schrems II: CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, p. 98-99.
[68] In the case Big Brothers the Court found that the methods of mass interception of communications practiced by the British Intelligence Agency violated article 8 and article 10 of the ECHR.
[69] CJEU, Judgment of the Court (Fourth Chamber) of 28 July 2016, JZ v Prokuratura Rejonowa Łódź – Śródmieście, Case C-294/16 PPU, ECLI:EU:C:2016:610.

How the ECtHR will respond to this, is not yet known, but the case Centrum för Rättvisa[70] and the case Big Brother Watch are challenged in the Grand Chamber now.

An assessment of the impact of the Schrems II on privacy protection is necessary in the scope of case law ECtHR, since all EU Member States are members of the Council of Europe and have signed the ECHR. The insufficiency in the dialogue of Courts hinders the formation of a coherent picture of protection in this area. In case of Digital Rights Ireland[71] the CJEU states the invalidity of the Directive 2006/24/EC. Referring to the case law of the ECtHR, the CJEU proceeded from the need for clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.[72] In the Schrems II there are no references to the case law of the ECtHR, and this is not accidental.

First, it is a response to the case Centrum and the case Big Brother Watch, which marked a certain departure from the "strict necessity" standard, recognizing the broad discretion of national authorities and approving the mass surveillance policy as a "valuable tool" for protecting national security.

Second, the EU through Schrems II shows itself as a strong actor in the sphere of human rights in the world. It shows that in this aspect, it is not very "bound" by the judicial practice of the ECtHR and can take the initiative in creating standards for the protection of human rights.

5. CONCLUSIONS

The judgment of the Schrems II case is not a mere continuation of the CJEU's approach about the legal standards of international data transfer and "extraterritoriality" of GDPR, which has already been expressed in Schrems I. Schrems II is an important decision with serious consequences that go beyond the direct impact on data transfer between the EU and the US. It is aimed at protecting EU data subjects from exceeding the national security powers of third countries, but it can also create many unresolved problems in the field of international data transfer. The Schrems II shows that the EU has an impetus for the development of a unique case law of CJEU regardless of the modern approach developed in the ECtHR.

The EU takes the initiative to protect human rights to privacy from state surveillance setting the tone with GDPR. But to protect people from mass surveillance, much more needs to be done. It is primarily a formulation of more harmonized global data protection standards, finding a balance between privacy and security, privacy and the economic dimension of international data transfer and so on. The modern case law of the CJEU can have important implications for strengthening the protection of human rights in Europe and curbing potentially dangerous changes for both human rights and economic situation. Perhaps in the future, the CJEU will be forced to develop a more balanced approach to the relationship between national security, privacy and economics. This is what the Schrems II lacks to create reliable legal instruments for international data transfer and harmonized global data protection standards.

We can conclude that the Schrems II is an important decision with serious consequences and can have controversial influence in the level of privacy protection in global level.

[70] ECtHR, Centrum v. Sweden, app. no. 35252/08, 19 June 2018.

[71] CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and KärntnerLandesregierung, Michael Seitlinger, ChristofTschohl and Others, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[72] Ibid., p. 54.

BIBLIOGRAPHY:

Advocate General's Opinions in case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreauxfrancophones et germanophone and Others, Press release No 4/20, 15 January 2020. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf (accessed on 18.11.2020).

European Commission. (2020a). Communication from the Commission to the European Parlament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. Retrieved 18 November 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

European Commission. (2020b). Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data. Retrieved 18 November 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

European Commission. (2020c). Coronavirus: EU global response to fight the pandemic. Retrieved 18 November 2020, from https://ec.europa.eu/commission/presscorner/detail/en/mex_20_631.

European Data Protection Board. (2020). Statement on the processing of personal data in the context of the COVID-19 outbreak. Retrieved 18 November 2020, from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

PRIVACY INTERNATIONAL. (2017). National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe/ Privacy International. Retrieved 18 November 2020, from https://privacyinternational.org/sites/default/files/2017-10/Data Retention_2017_0.pdf.

Scott, J. (2014). The new EU "extraterritoriality". *Common Market Law Review*, 51(5), 1343 – 1380.

The White House; Office of the Press Secretary. (2014). Presidential Policy Directive - Signals Intelligence Activities. Retrieved 18 November 2020, from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Untersinger, M. (2020). Europe requests data from telephone operators to assess the effect of containment measures. Retrieved 18 November 2020, from https://www.archyde.com/europe-requests-data-from-telephone-operators-to-assess-the-effect-of-containment-measures/.

Wiewiórowski, W. R. (2020). Monitoring spread of COVID-19. Retrieved 18 November 2020, from https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.

Annex I Safe Harbor Privacy Principles issued by the US Department of Commerce on 21 July 2000/, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (accessed on 18.11.2020).

CJEU, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559.
CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.
CJEU, Judgment of the Court (Grand Chamber) of 24 September 2019, Google Inc v Commision nationale de l'informatique et des libertés (CNIL), C-507/17, ECLI:EU:C:2019:772.
CJEU, Judgment of the Court (Fourth Chamber) of 28 July 2016, JZ v Prokuratura Rejonowa Łódź – Śródmieście, Case C-294/16 PPU, ECLI:EU:C:2016:610.
CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.
CJEU, Judgment of the Court (Grand Chamber) of 06 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650.
CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970
CJEU, Judgment of the Court (Grand Chamber) of 2 October 2018, proceedings brought by Ministerio Fiscal. Request for a preliminary ruling from the Audiencia Provincial de Tarragona, Case C-207/16, ECLI:EU:C:2018:788.
CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, The Investigatory Powers Tribunal (United Kingdom), in the proceedings Privacy International Case C-623/17, ECLI:EU:C:2020:790.
Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), C/2016/4176.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, p. 31–50.
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.
ECtHR, Big Brother Watch and Others v. United Kingdom, app. no. 58170/13, 62322/14 and 24960/15, 13 September 2018.
ECtHR, Centrum v. Sweden, app. no. 35252/08, 19 June 2018.
ECtHR, Szabó and Vissy v. Hungary, app. no. 37138/14, 12 January 2016.
ECtHR, Weber and Salavia against Germany, app. no. 54934/00, 29 June 2006.
ECtHR, Zacharov v. Russia, app. no. 47143/06, 04 December 2015.
Entscheidung des Bundesverfassungsgerichts - 1 BvR 2835/17 - (zu den §§ 6, 7, 13 bis 15, 19 Absatz 1, § 24 Absatz 1 Satz 1, Absatz 2 Satz 1, Absatz 3 des Gesetzes über den Bundesnachrichtendienst) (BVerfGE20200519 k.a.Abk.), 19.05.2020. Available at: https://www.buzer.de/gesetz/13986/index.htm (accessed on 18.11.2020).
Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield, Brussels, 13 April 2016. Available at: https://ec.europa.eu/justice/article-

29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf (accessed on 18.11.2020).
Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013
2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), Official Journal L 215, 25/08/2000, p. 0007 – 0047.
2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539).
2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Text with EEA relevance)