EXTRATERRITORIAL ENFORCEMENT DEFINED IN ARTICLE 3(2) OF THE GDPR: HOW EFFECTIVE?

1. Introduction

Majority of the processing of personal data is now subject to the Internet which eventually resulted in a disconnection from territorial scope of the data. In this respect, expanding the regional application of the data protection regulations has become inevitable. Extraterritorial jurisdiction of the GDPR and its enforcement is a case in the point.

The territorial scope of the GDPR is undertaken in the Article 3. According to Article 3(2), GDPR applies to a situation that the data controller or processor (hereinafter referred to as "**operators**") is not established in the Union, but targets the residents in the Union, if the related activity is about the offering of the goods and services, and monitoring behavior of the data subjects.[1] This refers to targeting criterion which will be the main focus of this essay.

Given the fact that operators who are established outside of the EU, but processes data of the individuals located in the EU, obliged to comply with the GDPR and their national data protection standards. Therefore, the new territorial scope of the law has raised the issues of effective enforcement of the provision outside of the EU. This essay will first discuss the uncertainties lies under the Article 3(2). Then it will move on to evaluate the extraterritorial enforcement of the supervisory authority's orders with a discussion of their effectiveness. Finally, the concept of representation as an enforcement tool will be examined.

2. Uncertainties concerning the extraterritorial application of the Article 3(2)

The determination of whether the data operators actually aim individuals located in the EU is a controversial topic.[2] Two of the concepts provided under the Article 3(2) is offering goods and services, and monitoring behaviors.[3] Frame of the article has been specified through some criteria provided by the case law. For instance, accessibility of a website in a certain area is not a conclusive factor regarding determination of the targeted individuals.[4] While appointing the targeted consumers, court has considered the factors listed under the Recital 23 such as involvement of one of the EU language or a mention of the EU consumers. In addition, monitoring behavior on Internet is not enough and predicting their possible future behavior and using it for planning is mandatory.[5] Even though some specifications have been made,

[1] GDPR, art 3(2).
[2] Svantesson, Dan Jerker B., Stockholms universitet, Institutet för rättsinformatik (IRI), et al. 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation', International Data Privacy Law, vol. 5/no. 4, (2015), pp. 226-234.
[3] GDPR, art 3(2)(a)-(b).
[4] Joined Cases C-585/08 and C-144/09 Pammer and Hotel Alpenhof [2010] I-12527, para 69.
[5] Greze, Benjamin. 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives', International Data Privacy Law, vol. 9/no. 2, (2019), pp. 109-128, 114.

there is an ambiguous line between the activities aiming global and only EU which necessitates a case-by-case evaluation.[6]

It is clear that Article 3(2)(a) and (b) needs more clarification and guidance through case law. Indeed, ambiguous nature of the provision negatively impacts the right to legal certainty which refers to "know your rights through accessible and foreseeable legal provisions".[7] This also a concern of the data operators, given the fact that if their activities fall under the scope of the GDPR, high financial sanctions would be imposed. On one hand, if determined penalties are enforceable, the territorial area of the enforcement is lack of certainty.[8] On the other hand, if the penalties cannot be enforceable, the legal system as a whole would be harmed.[9]

3. Extraterritorial enforcement of EU supervisory authority's orders

EU supervisory authorities have certain power to exercise within the territorial scope offered under Article 3. However, when it comes to imposing orders of the EU authorities, cross-border complexities occur in the means of enforcement. One of the main case law regarding the jurisdiction is the Lotus case. Principle set out under this case is that "jurisdiction is certainly territorial".[10] The only exception could be a rule originated from an international custom or a convention.[11]

However, states still have the power to claim jurisdiction of their courts on the cases which has occurred outside their territory, since international law composed principles to put this power into practice. However, imposing GDPR over a data operator located in a non-EU country is not that simple.[12] This is mainly because the third state may not allow the enforcement of the law, by the idea of sovereignty of foreign state.[13] Even though GDPR seeks to enforce its provisions, the concept of non-interference in the affairs could prevent to reach that objective.[14]

4. The non-enforcement of foreign public laws

[6] de Hert, Paul, and Michal Czerniawski. 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context', International Data Privacy Law, vol. 6/no. 3, (2016), pp. 230-243, 240.
[7] Ibid.
[8] Kuner, C. 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', International Journal of Law and Information Technology, vol. 18/no. 3, (2010), pp. 227-247, 234.
[9] Ibid, 235.
[10] SS Lotus (France v Turkey) 1927 PCIJ paras 41–47.
[11] Ibid.
[12] Kuner, C. 'Data Protection Law and International Jurisdiction on the Internet (Part 1)', International Journal of Law and Information Technology, vol. 18/no. 2, (2010), pp. 176-193, 188.
[13] Ibid.
[14] Ibid.

According to Article 58(5), supervisory authority may engage in legal proceedings in order to enforce GDPR provisions against an organisation located outside of the EU.[15] In this regard, recourse to an EU court and recourse to a foreign court must be examined. First of all, recourse to an EU court is pointless, since the organisation is not EU based. An order of a data protection authority cannot be enforced outside the EU borders, unless otherwise has been agreed with a third country.[16] Secondly, the recourse to foreign court is not an effective option because if that state has a data protection law, there is a great possibility of conflicts of law issue.[17]

Since GDPR aims to protect fundamental rights and freedoms of individuals, particularly by protecting their personal data,[18] it can be classified as a public law. "The result is that a foreign court will not exercise its own jurisdiction merely in aid of the lacking enforcement jurisdiction of an EU court", therefore, breach of GDPR by a data controller located in non-EU country cannot be bring to the court.[19] As a result, an effective implementation of the provisions such as imposing sanctions and the enforcement of an EU supervisory authority's decision will only depend on the free will of the data controller.

5. Enforcement through designation of a representative

The extraterritorial scope of Article 3(2) is confronting with enforcement problems. One of the enforcement tool to overcome the problems is the designation of a representative by the data operators. In the case that data operators are subject to the GDPR, but has no establishment in the EU, an operator shall designate a representative in the EU,[20] unless the activities of the operator are occasional.[21] The role of the concept is to represent data operators regarding the obligations determined under the GDPR.[22] The aim of the provision is to expand the territorial scope of the GDPR's implementation and ensure the compliance of data operators with the law.[23] However, this has also raised concerns regarding the enforcement issues.

According to the Article 27(5) it is stated that designation of a representative cannot prevent any legal actions that could be initiated against the data operators located in a non-EU country.[24] When this is the case, the question of whether the representative is subjected to any liability as a result of a breach of the GDPR has become an issue.[25] There is a controversy as

[15] GDPR, art 58(5).
[16] Ibid (n 5) 115.
[17] Ibid.
[18] GDPR, art 1(2).
[19] Ibid (n 5) 116.
[20] GDPR, art 27(1).
[21] GDPR, art 27(2)(a).
[22] GDPR, art 4(17).
[23] GDPR, art 27(4).
[24] GDPR, art 27(5).
[25] Azzi and Adèle, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation" (JIPITECOctober 23, 2018) pp 126-137, 133.

to the answer, since no specified provisions or court orders have been provided to compose a uniform answer.

On one hand, Article 27 is silent about addressing a person for liability in the event of noncompliance with the GDPR. On the other hand, recital 80 indicates that the representative of the operator "should be subject to enforcement proceedings", however it had failed to provide an enforcement mechanism. Furthermore, the European Data Protection Board defended that the equity of the statute aims to form a liability structure for the representative in a similar way as an operator.[26] Although the interpretation appears to set liabilities for representatives, this is not enough to hold penalties for any breach, since GDPR is not addressing representatives for obligations specified for operators.[27] For instance, in case of requesting information, the lawmaker has explicitly entitled the representative for such an obligation.[28] Therefore, considering that there is no reference about the liability under the GDPR, it is possible that lawmaker has intentionally avoided determining liabilities for representatives.

Pursuant to the statement of Article 29 Working Party, sanctions and enforcement against representative depend on the law of the Member State in which representative is located.[29] For instance, according to Belgium law, civil liabilities are stated for representative, however, in other Member States there is no such clear provisions.[30] Considering the fact that data operator is free to choose any of the Member States that he is performing activities for designation,[31] the initial idea of the operator would be deciding on a Member State law that creates no or less liability. This has referred to as "forum shopping"[32] which is an undesired outcome since it prevents the fair implementation of the GDPR.

It is clear that designating a representative does not indicate any benefit for enforcement purposes. The result would be imposition of the sanctions which cannot be enforced outside the EU. Given the fact that cross-border complexities in the enforcement area, representation of the data operator could be a notable concept. However, the weak appeal of the current situation may cause a discouragement in designating a representative. In order to eliminate the enforcement problems, an advantageous route should be drawn. For instance, according to the Working Party "the mere presence of a representative in a Member State does not trigger the one-stop-shop system" which means that operators located outside the EU must deal with

[26] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation' (16 November 2018) 23 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf> accessed 10 April 2020.
[27] Ibid (n 25) 133.
[28] GDPR, art 58(1)(a).
[29] Article 29 Working Party, 'Opinion 8/2010 on Applicable Law' (16 December 2010) WP 179, 23.
[30] Ibid (n 5) 124.
[31] GDPR, art 27(3).
[32] Ibid (n 25).

each of the authority they are performing.[33] In exchange for that, it could be agreed that liability of the representatives for infringement of the GDPR is possible.[34] Consequently, an artificial bound would be established between the EU and third countries which results in a rise in the effectiveness of the GDPR outside the EU.

6. Conclusion

The territorial scope is now aiming to reach the organisations outside the EU by enforcing the provisions and orders. However, the article itself is creating an ambiguity on which non-EU organisation will fall into the scope. Even though data operators discover that they should comply with the GDPR, territoriality and sovereignty principles are not permitting to enforce the law outside the EU. Finally, GDPR has suggested a tool for enforcement purposes which is designation of a representative. However, because of the indecisive nature of the GDPR has caused failure of entitling liability to the representative which made the concept ineffective.

Initial aim of the GDPR is to protect the personal data of the individuals located in the EU. However, it is clear that GDPR is going beyond its aim and becoming a global data protection regulation due to the extraterritoriality effect. Some businesses comply with the standards and orders in order to create a well commercial reputation and avoid the relevant damage it could cause. Some do not have any concern about noncompliance because of the ineffective enforcement mechanism. Thus, extraterritorial impact does not reveal a real power and seems an illusion.

[33] Schmitz S, "European Union · The Article 29 Working Party's Guidelines for Identifying the Lead Supervisory Authority in Cross-Border Data Processing" (2017) 3 European Data Protection Law Review 90

[34] Ibid (n 5) 125.